مدخل

الى الامن السيبراني



تاليف الدكتور

محمد محمود العمري

مدخل

إلى الأمن السيبراني

تأليف

الدكتور محمد محمود العمري

2020م

الطبعة الأولى

1441هـ-2020م

المملكة الأردنية الهاشمية

رقم الإيداع لدى دائرة المكتبة الوطنية

العمري ، محمد محمود

مدخل الى الامن السيبراني / محمد محمود العمري .- عمان: دار زهران للنشر والتوزيع، 2020.

(   ) ص.

ر.أ. : (2020/2/738)

الواصفات: /الامن المعلوماتي //حماية البيانات /الجرائم الحاسوبية /السرية /الامن القومي /البلدان العربية /

- أعدت دائرة المكتبة الوطنية بيانات الفهرسة والتصنيف الأولية.
- يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى.

الرواد والمرجع الأصدق للكتاب الجامعي والأكاديمي

دار زهران للنشر والتوزيع

تلفاكس : 5331289 – 6 – 962+، ص.ب 1170 عمان 11941 الأردن

E-mail : Zahran.publishers@gmail.com

الإهداء ...

إلى تلك الشيبات الطاهرة ومن يحملها (والدي العزيز)

إلى الأصل والطيبة وبركة الدعاء (والدتي العزيزة)

إلى رفيقة دربي المخلصة ومصدر إلهامي (زوجتي

إلى فلذات كبدي وسند (أبنائي)

إلى عزوتي (أخواني وأخواتي)

إلى ثرى وطن الأردن ... بما ضمت من اربد إلى عمان...

إليهم جميعاً أهدي جهدي وباكورة أعمالي.

المؤلف

الدكتور محمد محمود العمري

فهرس المحتويات

قائمة الجداول والأشكال

المقدمة:

شهد العالم تطوراً متسارعاً في مجالات الحياة كلها، ومن هذه المجالات التي لم تخرج من دائرة التطور، قطاع الاتصالات وتقنية المعلومات، في هذا العالم لم تعد الحدود بين الدول حاجزاً، ولم تعد المسافات معضلة في التواصل، أصبح الإنسان ينجز أعماله من بثواني عبر حاسوبه أو هاتفه، وظهرت مفاهيم جديدة لم تكن موجودة ومنها السيبرانية، وهو مفهوم جديد ويحمل في طياته الكثير من الأمور التي تستحق البحث والدراسة، وتنبهت الدول إلى أهمية هذا المفهوم والتعامل معه بجدية، حيث ارتبط هذا المفهوم بافتتاح المراكز البحثية وبدأ الباحثين يكتبون في هذا الشأن، كما قامت الدول بسن القوانين والتشريعات التي تتوائن مع هذه المرحلة، كل ما ذكرنا هدفه حفظ الأمن للأفراد والدول، ذلك أن ما يتنعم به الإنسان بفضل الثورة السيبرانية، لم يكن نعيماً مطلقاً، بل بدأت تتكشف مخاطر أمنية على الأفراد والدول تستدعي التنبه لها.

تأسيساً على ما سبق لا بد من أن ندرس ما أمكن عن هذا المصطلح (السيبرانية) وغيره من المصطلحات المرتبطة به (الفضاء السيبراني) (الأمن السيبراني) (الإرهاب السيبراني) (الهجمات السيبرانية) (الجريمة السيبرانية)، نلاحظ من النظرة الأولى أن هذه المصطلحات تستهدف الدول والأفراد، وتنعكس على الاقتصاد والمؤسسات والمجتمعات وقيمهم وأخلاقهم، ونظراً لما لهذا الموضوع من أهمية وضع المؤلف هذا الجهد المتواضع، والذي يعتبر من الدراسات الحديثة والمواضيع التي ما زالت مكتباتنا العربية تفتقر إليها، ويأمل المؤلف أن يستفاد من مواضيع الكتاب للباحثين وطلبة الجامعات والمهتمين بالسيبرانية والله الموفق.

المؤلف

الفصل الأول

الأمن السيبراني

المبحث الأول

مفهوم السايبر ونشأته ومفاهيم مرتبطة به

(النشأة، الخصائص، الأبعاد)

مقدمة:

إن الأمن هو ضرورة من ضروريات الحياة منذ نشأة الخليقة، والدول تسعى وبشتى السبل إلى المحافظة على ديمومتها واستمراريتها، ويكون ذلك من خلال تعزيز مجموعة من المقومات المترابطة منها السياسية والاقتصادية والاجتماعية والعسكرية ومع تطور التكنولوجيا وظهور أخطار جديدة رافقت هذا التطور، ولم تكن موجودة في الماضي أصبحت الدول بحاجة ماسة إلى مجاراة مستجدات العصر ومنها التكنولوجي، والاستعداد لأي خطر يمس سيادتها وأمنها القومي، ومن ذلك سارعت دول عديدة مع نهايات القرن العشرين وبدايات القرن الواحد والعشرين إلى وضع ملف جديد على أجندتها السياسية ألا وهو الأمن السيبراني، لا سيما وأن ثورة المعلومات والاتصالات، قد زادت من نسبة الخطر السيبراني، ذلك أن الاقتصاد والأمن والاتصالات مرتبطة بشكل وهو ما دعا الساسة وأصحاب القرار والمختصين يدركون أنه لا يمكن فصل أمن الفضاء السيبيري، والاقتصاد والأمن القومي في الدولة.

ونشير إلى ذلك ما عبر عنه المسؤول السابق عن الأمن الوطني الأميركي، مايكل ماكونال، " أن الإنترنت، قد رفعت مستوى الأخطار التي يتعرض لها النظام، بشكل غير مسبوق" (الموقع الإلكتروني، McConnell said the Internet has). وبالعودة قليلاً إلى بداية القرن الواحد والعشرين نجد أن الرئيسي الأميركي السابق، باراك أوباما، أعلن

صراحة أن أمن الفضاء السيبيري، يأتي في مقدمة اهتماماته، ومعتبراً التهديد الآتي من الفضاء السيبيري، من أخطر المسائل، التي تطرح على المستوى الاقتصادي، وذلك وعلى مستوى الأمن القومي. وقام بخطوات جادة تطبيقاً لتصريحاته، بتعيين مسؤول عن أمن الفضاء السيبيري، يكون على اتصال وتنسيق دائمين معه، ويكون عضواً في الأمن القومي، وفي المجلس الاقتصادي الوطني (الموقع الإلكتروني، Loppsi en France et Cyber-securite aux USA).

ولقد اتجهت دول عديدة نحو اتجاه الولايات المتحدة الأمريكية والدول العربية منها، وذلك للقناعة التامة لهذه الدول أن ما نتج من ثورة تكنولوجية مفيدة للبشرية رافقها ظهور تهديدات وجرائم سيبرانية، أصبحت تشكّل تحدياً كبيراً للأمن القومي للدول وكذلك سلامة الأمن الدولي، ولا بد من وجود ضمانات أمنية ضمن هذه البيئة الرقمية المعقدة، والتي كان نتاجها ظهور الأمن السيبراني (cyber security) كبُعد جديد ضمن أجندة حقل دراسات العلاقات الدولية والاستراتيجية والسياسية والأمنية وكضمان امني في البيئة الرقمية.

تأسيساً على ما سبق سيقوم المؤلف في الفصل الأول من هذا الكتاب بدراسة معمقة لمواضيع الأمن السيبراني والمفاهيم المرتبطة به ودراسة نشأته وخصائصه وأشكال الجريمة السيبرانية ومخاطرها والتي ستشكل لدى القارئ معرفة لباقي فصول الكتاب نظراً لأهميتها والحاجة إلى دراستها والإلمام بها .

المطلب الأول

السيبرانية في اللغة والاصطلاح

سيتم تقسيم هذا المطلب إلى ثلاثة فروع: الفرع الأول يبحث في الأصل اللغوي لكلمة السيبرانية، أما الفرع الثاني فيركز ويحدد على التعاريف الاصطلاحية لمفاهيم السيبرانية، وما ارتبط بها من مفاهيم حسب وجهات نظر المختصين والعلماء المختلفة، والفرع الثالث سيبحث في نشأة وتطور الأمن السيبراني.

الفرع الأول: مصدر كلمة سايبر (Cyber) في اللغة

تجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصل كلمة سايبر إلى عالم الرياضيات الأمريكي (norbert wieners 1894-1964) م، وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير(Cybernetics or control and communication in" the Animal and the machine) : وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب. (Norbert Wiener, 1948.)

وفي ما يلي وبعد البحث في القواميس اللغوية العالمية ما جاء من تعريف أو ذكر عن أصل كلمة سايبر (Cyber).

- قاموس أكسفورد: جاءت ككلمة يونانية الأصل وتعود إلى مصطلح (kybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بُعد (Julia Cresswell, 2010).
- قاموس (المورد): وردت كما يلي " السيبرانية: هي علم الضبط، ومصدرها (Cybernetics)" (البعلبكي، منير، المورد، 2004م، ص243).
- قاموس المصطلحات العسكرية الأمريكية يعرفها: "أي فعل يستخدما عن طريق شبكات إلكترونية بهدف السيطرة أو التعديل لبرامج إلكترونية أخرى" (U.S. Department of Defense, 2012).
- قاموس مصطلحات الأمن المعلوماتي، السيبرانية هو: هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى

محميـة إلكترونيـاً لتعطيلهـا أو تـدميرها أو الأضرار بهـا"(Richard Kissel, 2013, p.57) .

وفي اللغة العربيـة يتبـين بعـد البحـث المعمـق أنـه لا يوجـد مصـطلح مناظر لكلمة سايبر في اللغة العربية، كما أن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استخدمت مصطلح السيبراني نفسـه، وذلـك لأن هـذا العلـم حديثاً، ولم ينشأ في الوطن العربي، وإنما يدور وجوداً وتطوراً في العالم الغـربي. (للاطلاع: أنظر، الموقع العربي: مكتب الأمم المتحدة)

وقبل الانتقال إلى الفرع الثاني والـذي سيشـمل التعريـف الاصـطلاحي لعدة مفاهيم ونظـراً لأنـه سـيتم اسـتخدام كلمـة "الأمـن" لاحقـاً فـلا بـد مـن تعريفها ولو بشيء من الإيجاز حيث يعرف الأمن بأنه: الأمـن مـن آمـن يـأمن أمناً؛ فهو آمن، وآمن أمناً وأماناً، اطمأن ولم يخف، فهو آمن وأمن وأمين، والأمن يعني الاستقرار والاطمئنان، نقول: أمن منه أي سلم منه، وأمن علـى مالـه عنـد فلان أي جعله في ضمانه، والأمان والأمانة بمعنـى واحـد، فـالأمن ضـد الخـوف، والأمانة ضد الخيانة، والمأمن الموضع الأمن (ابن منظور، لسان العـرب، 2000م: ص163)، وقد عرّفه قاموس بنغوين للعلاقات الدوليـة بأنـه مصـطلح يشـير إلى غياب ما يُهدد القيم النادرة، كما يعرف الأمن: " إحساس بالطمأنينة يشـعر بـه الفـرد، سـواء بسـبب غيـاب الأخطـار التـي تهـدد وجـوده، أو نتيجـة لامتلاكـه الوسائل الكفيلة بمواجهة تلك الأخطار حال ظهورهـا". (زهـرة، عطـا محمـد، في الأمن القوم العربي، 1991م)

الفرع الثاني: التعاريف الاصطلاحية لمفاهيم السايبر (Cyber)

تعددت المصطلحات والمفاهيم المستخدمة والمرتبطة بكلمة سايبر حيث تبنى المختصين مصطلحات انبثقت من كلمة سايبر كل حسب اتجاهه وتخصصه وفيما يلي أهم وأبرز ما جاء من تعريفات :

- **مصطلح الأمن السيبراني (Cyber Security) :**

- عرفه التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الإصلاح في الاتصالات للعام 2010-2011م"، بأنه: مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين(Trends in Telecommunication Reform, 2010).

- عرفه الكاتبان (Neittaanmäki Pekka,Lehto Martti) في كتابهما Cyber Security: Analytics, (Technology and Automation) أنه: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة".

- بينما عرّفه إدوارد أمورسو (Amoroso Edward) بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات

المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة".

- أما وزارة الدفاع الأمريكية "البنتاغون" وضعت تعريفاً دقيقاً لمصطلح الأمن السيبراني، فاعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث".
- في حين اعتبر الإعلانُ الأوروبي الأمنَ السيبراني أنه:" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".

ويرى المؤلف أن تعريف وزارة الدفاع الأمريكية (البنتاغون) هو الأقرب إلى الواقع، وذلك بأنه تحدث عن " جميع الإجراءات التنظيمية"، ولم يقتصر الإجراء على جانب محدد من جوانب الحماية المعلوماتية، إضافة إلى أنه لم يفرد حماية خاصة لكل جانب من جوانب المعلومات، وإنما شملها جميعاً سواء كانت هذه المعلومات تتعلق بالبيانات أو المعتدية او بالمحتوية المادي للأنظمة المعلوماتية، إضافة إلى أنه لم يحدد جريمة سيبرانية بعينها، وإنما شمل طوائف الجريمة السيبرانية جميعها حسب الهدف والغاية من ارتكابها.

- **مصطلح الفضاء السيبراني (Cyber Space) :**

المحيط الذي تجري فيه العمليات السيبرانية (Cyber Operations) الناشئة عن أداء أنظمة إلكترونية مهمتها متابعة وجمع المعلومات التي تعمل إلكترونياً وتحليلها ومن ثم

اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة إلكترونية أخرى مخصصة لهذا الغرض (James, A.Lewis, " 2010, P56).

- عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI):" فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" .

– **مصطلح الردع السيبراني (Cyber Deterrence):**

- "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"، ويرتكز الردع السيبراني على ثلاث ركائز هي عماد استراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع (Credible Defense)، والقدرة على الانتقام(An Ability to Retaliate)، والرغبة في الانتقام (A Will to Retaliate).

– **مصطلح الجريمة السيبرانية (Cyber Crime):**

- "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها".

- مصطلح القوة السيبرانية (Cyber Power):

- يعرف جوزيف. س ناي (Nye.S Joseph) بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية".

- مصطلح الهجمات السيبرانية (Cyber Attacks) :

- عرفت القيادة الاستراتيجية الأمريكية (U.S. Strategic Command)، الهجمات السيبرانية بأنها: " تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعّال لها، فضلاً عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها" (K. Saalbach, op. cit. p8).

- شين (Shin) حيث يعرفها: "استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها " (Shin. Beomchul, op. cit. p 105).

- فيورتس (Fuertes) ويرى أنها: " هجوم عبر الإنترنت يقوم عل التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى (Micheal S. Fuertes, 2013, p1).

- كما عرفها شمت (Schmitt) بـالقول: "مجموعـة مـن الإجـراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهـدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظـم المعلومـات الخاصة بالدولـة المهاجمـة". (Schmitt, M.N, 1999, Vol, 27, No, 885-937. P7).

- تعريـف زيمـت وبـاري (Zimet & Barry) : " مجموعـة مـن العمليات القائمة على الحرب الإلكترونية والخـداع الـنفسي، فضـلاً عن استهداف شبكة تواصـل العـدو العسـكرية وعملياتـه الأمنيـة الإلكترونية (Zimet. E. and C. L. Barry, 2009, p 291).

- مـــاركو روســـيني (Matco Roscini): "تطويـــع الإمكانيـــات الإلكترونيـة العسـكرية لأجـل التـأثير في مواقـع إلكترونيـة أخـرى وتعطيلهـا أو تـدميرها سـواء أكانـت تقـدم خـدمات مدنيـة أو عسكرية" (Marco Roscini, 2010, p91).

الفرع الثالث: نشأة الأمن السيبراني

شهد العالم في القرنين العشرين والحادي والعشرين ثورة تكنولوجية متسارعة، رافقها انعكاسات على جميع مجالات الحياة البشرية، ومع هذه الثورة التكنولوجية ظهرت مصطلحات ومفاهيم جديدة، منها ما كان مرتبطاً بالجانب الإيجابي للتكنولوجيا ومنها الجانب السلبي والمخيف أيضاً، وبدأت الدول من جهة والمفكرين والعلماء من جهة أخرى في البحث والدراسة للوقوف على كل جانب إما بتعزيز قوتها (الاقتصادية والعسكرية) ونهضتها أو بدرء الأخطار المحتملة للمحافظة على أمنها واستقرارها، ومن ذلك السيبرانية بمفهومها العام والسعي إلى تحقيق الأمن السيبراني.

وفي دراسة نشأة الأمن السيبراني نجد أن معالمها تلازمت بمرحلتين نوعيتين تاريخياً:

- **المرحلة الأولى:** منتصف الخمسينات من القرن العشرين واستحداث أجهزة الكمبيوتر كأداة لمعالجة وحفظ المعلومات رقمياً (Digital)، وما ترافق من جهود عدد من الشركات الخاصة والعامة، حيث توجت هذه الجهود بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، واستمر هذا التطور ليصبح جهاز الكمبيوتر من أساسيات العمل لدى الشركات والأفراد لما في ذلك من توفير للجهد والوقت. (Christopher. Joyner and Catherine Lotrionte, 2001. P.825).

المرحلة الثانية: وهي فعلاً ثورة تكنولوجية غيرت مجرى الحياة البشرية، ألا وهي ظهور شبكة الانترنت، حيث وفي ثمانينيات القرن

الماضي، قادت الأبحاث التي أشرف عليها السير (تيم بيرنرز لي في المنظمة الأوروبيّة للأبحاث النوويّة (CERN) إلى تطوير شبكة الويب، ونتج عن ذلك ربط مُستندات النص التشعبي بنظام معلومات يُمكن النفاذ إليه من أي موقع على الشبكة، ومنذ مُنتصف التسعينيّات كان لشبكة الإنترنت تأثيرٌ ثوريّ على الثقافة والتجارة والتكنولوجيا، وشمل ذلك ظهور التراسل الفوري وتطوّر البريد الإلكترونيّ والمُكالمات الهاتفيّة عبر شبكة الإنترنت (VoIP) ومكالمات الفيديو وشبكة الويب التي تضمنت مُنتديات النقاش وشبكات التواصل الاجتماعيّ ومواقع التسوّق عبر الإنترنت.. . (Nick Couldry 2012, p2)

ولقد رافق تلك الثورة انعكاسات على الجانب العسكري والتسلح لدى الدول، وأطلق البعض على ذلك مصطلح الحرب السيبرانية الباردة (Cyber Cold War) أو سباق التسلح السيبراني Cyber arms race). (Tang Lan, Zhang Xin, Hatty D.) . (.Reduege, Jr., p1

ونجد أنه أول ما نشأ في مجال السيبرانية هو الجريمة السيبرانية، حيث كانت على شكل جرائم وجهها الجناة تجاه المؤسسات المالية والمصرفية، أضف إلى ذلك الشركات المتخصصة ببرمجة نظم الاتصالات، وقد سارعت بعض الدول اتخاذ المواجهة والإجراءات التشريعية والقانونية لتجريم الأفعال وتحديد العقوبات (الموقع الإلكتروني)، وسنتعرف على تلك الإجراءات في فصل لاحق مستقل من هذا الكتاب.

وما لبث أن اتجهت الأنظار وخصوصاً في علم العلاقات الدولية إلى هذا التطور والأخذ به كمصدر قوة وسلاح جديد وأصبح الباحثون يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي، ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة (power)والسيادة (sovereignty) والحوكمة العالمية (global governance) والأمنية (securitization).

وعلى نفس الصعيد ظهر الاهتمام بالدراسات والأبحاث القانونية المهتمة بمجال الهجمات السيبرانية، حيث يعد كل من الباحثان جون اركويلا (John Arqyile) وديفيد رونفليد (Davied Ronfeld) أول من تعمقاً في البحث في مسألة الهجمات السيبرانية وذلك في العام 1997م، في كتابهم "الحرب السيبرانية قادمة" (cyber war is Coming)، حيث نجد أنهما تنبهان إلى أنظمة الاتصال الإلكترونية ودورها في النزاعات المسلحة مستقبلاً. (Arguilla, J and D.Ronfeld, 1997, p.59)

ولن نخرج عن الإطار السياسي وارتباطه بالأمن السيبراني، نظراً لأهميته دولياً حيث كان لرؤساء الدول الكبرى رؤية أمنية واستراتيجية في هذا المجال، إذ اعتبرت بعض الدول القدرة السيبرانية لديها يستحق الكتمان باعتباره عنصر أساسي من عناصر الأمن القومي، لكن ومع ازدياد وتيرة التطور في هذا المجال قام عدد من أصحاب القرار والمسؤولين في دول العالم بالاستعداد لمواجهة المخاطر الناتجة عن هذا التطور، ولكي لا يبقى أن الأمر لم يبق على هذا النحو، فسرعان ما أبدى قادة دول ومسؤولون عن رغبتهم في تطوير ورفد الدعم للجانب السيبراني انطلاقاً من

المبـدأ المعـروف (الـدفاع عـن الـنفس) (Self - Defense). (Yoram Dinstein, 2002, pp. 114-115).

ونذكر هنا ولو بشيء مـن الإيجـاز عـدداً مـن الأمثلـة تعزيـزاً للسـطور الأخيرة من الفقرة السابقة:

- في عـام 2003م اقـترح رئـيس قسـم الحـرب الإلكترونيـة الصـينية، داي كـوينجمن، بأنـه: "..... عـلى الصـين أن تتهيـأ لحـرب سـيبرانية تتضـمن سلسـلة هجـمات إلكترونيـة، مـا يـدعوها إلى الإعـداد والتنسـيق في العمليات العسـكرية لصـد الهجـمات السـيبرانية المضـادة ..." (Larry Wortzel, 2009).

- في العام 2009م صرح الرئيس الأمريكي السابق باراك أوباما قـائلاً : " ... وبالتالي فـإن الفضـاء السـيبراني هـو حقيقـة ومخـاطرة قادمـة معـه لا محالة..." (الموقع الإلكتروني).

صرح أيضاً: " لم نستعد كما يجب، بل فشلنا في تـأمين الحمايـة الكافيـة للبنى التحتيـة الرقميـة الخاصـة بنـا" (الموقـع الإلكـتروني، President Obama's Remarks on Securing, 2009).

في العام 2000م أدلى الرئيس الروسي فلاديمير بوتين بتصريح يتعلق بتعاليم أمن المعلومات (Information Seeurity Doctrine) حيث قام كل من جادي (Gady) واوستن (Austin) بتحليل ما صرح به في كتابهما (روسـيا والولايـات المتحـدة والدبلوماسـية ...)، وملخـص ذلـك بمـا يـلي: " زيـادة المخاطر السيبرانية التي تتعرض لها روسيا مقابل تخصيصات ماليـة قليلـة

حالياً مخصصة لدعم برامج الدفاع السيبراني"، ومن ثم وضع بوتين برنامج طويل الأمد لتطوير قدرات روسيا، وبما يتناسب وحاجتها لمنظومات الاتصال الإلكترونية وتسخيرها في الجانب العسكري والأمني". (Franz-Stefan Gady and Greg Austin, 2010, p.1.1)

- في العام 2010م وفي كلمة له صرح زعيم حزب المحافظين في بريطانيا، ديفيد كاميرون (كيف يمكن لبريطانيا أن تتصدى بشكل أفضل لتهديدات القرن الحادي والعشرين) قائلاً: " سيكون الأمن السيبراني الجزء الأهم ضمن استراتيجية الحزب على الصعيد القومي". (الموقع الإلكتروني، David Cameron, 2010)

ومما يؤكد تزايد أهمية الأمن السيبراني من وجهة نظر استراتيجية الولايات المتحدة الأمريكية إحصائية لورود كلمة(Cyber) في تقارير استراتيجية الأمن القومي الأمريكي لرؤساء الولايات المتحدة الأمريكية من العام 1998م إلى 2017م، وكما هو مبين بالجدول رقم (1).

السنة	الرئيس	عدد مرات ورود كلمة (Cyber)	سياق ورود الكلمة
1998	كلينتون	04	حماية المنشآت الحيوية، الجريمة، التعاون الدولي
2000	كلينتون	10	حماية المنشات الحيوية، الجريمة، التعاون الدولي، تبادل المعلومات، المرونة السيبرانية

السنة	الرئيس	عدد مرات ورود كلمة (Cyber)	سياق ورود الكلمة
2001	كلينتون	08	التهديدات الدولية,الحروب اللاتماثلية، المعلومات، المرونة السيبرانية
2002	بوش الابن	00	لا شيء
2006	بوش الابن	01	عسكرة الفضاء السيبراني
2010	اوباما	22	الدعم العسكري، الأولوية العالمية، الشراكة، الإرهاب، الوعي
2015	اوباما	19	التجسس السيبري، القواعد، المنشآت القاعدية، تنامي التهديدات، عسكرة الفضاء السيبراني، الوعي، الشراكة
2017	ترامب	41*	الفواعل، الفضاء السيبري، التدريبات والفرص، العصر السيبراني، الجريمة، الهجوم، المنشآت القاعدية، القدرات، الأمن السيبراني

الجدول رقم (1) المصدر:

https://www.tripwier.com/state-of-security/goverment

المطلب الثاني

أهمية الأمن السيبراني وفواعله

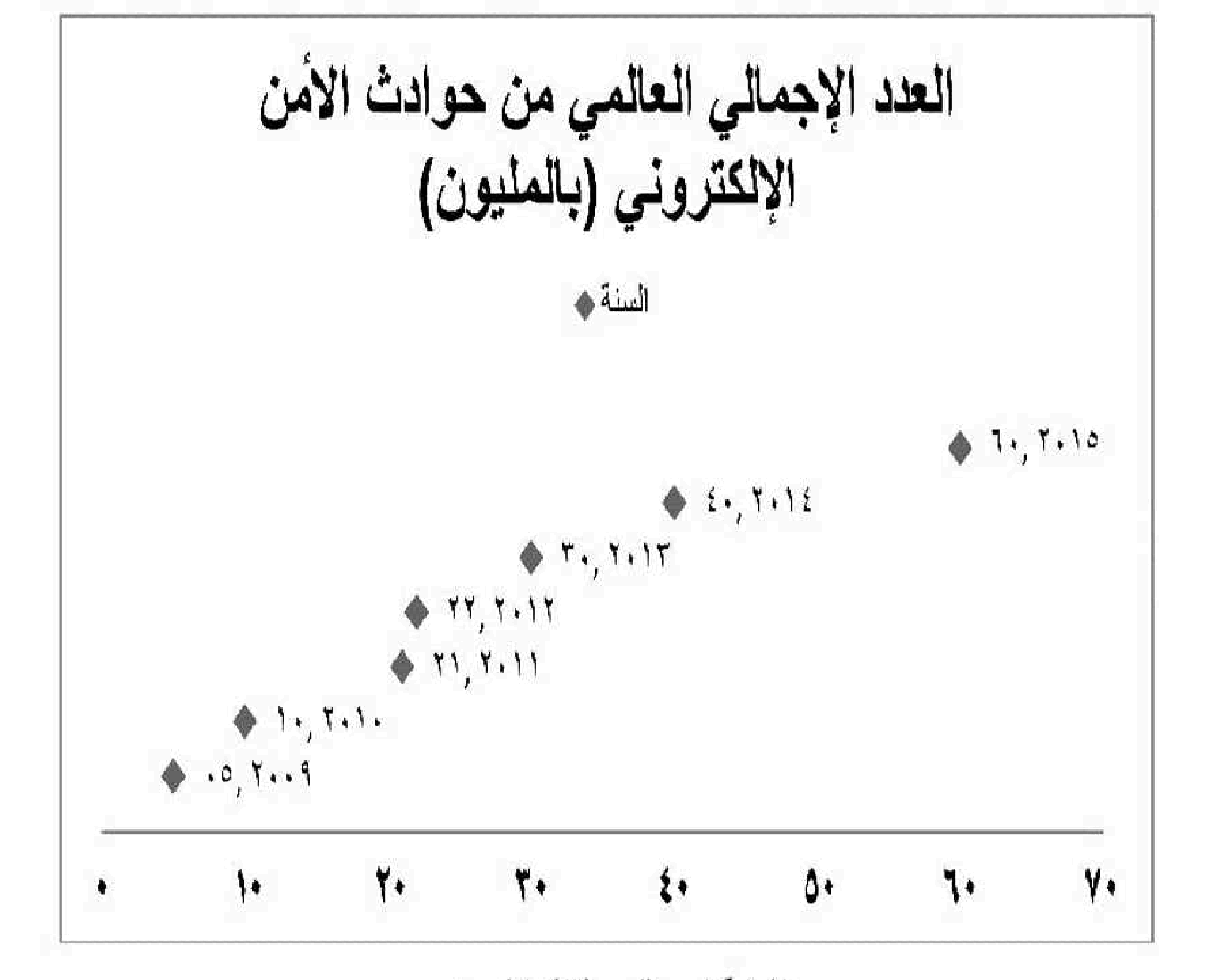
الفرع الأول: أهمية الأمن السيبراني

تتجلى أهمية الأمن السيبراني مع تزايد اعتماد الأشخاص حول العالم على التكنولوجيا ووسائل الاتصالات الحديثة الحديثة، حيث أصبح الأفراد والمؤسسات والدول أكثر عرضة للهجمات الإلكترونية، وعلى صعيد الدول نشير أنه كلما شهدت البنية التحتية للدول تقدما ملحوظاً في مجال تكنولوجيا المعلومات، فإن أمنها الوطني سوف يظل عرضة للمخاطر، وذلك من خلال مدى قدرة الجماعات الإرهابية على شن هجمات سيبرانية على قطاعي الدفاع والأمن، أيضاً تستغل الجهات الفاعلة إلكترونياً وكذلك الدول القومية نقاط الضعف لدى خصومها لسرقة المعلومات والأموال وتطوير القدرات لتعطيل وتدمير أو فقط تهديد قدرة دولة الخصم على تلبية الخدمات الأساسية، أما على صعيد الأفراد والمؤسسات فهم عرضة للهجمات العديدة مثل اختراق أمن الشركات، والتصيّد الاحتيالي، وممارسة الابتزاز والنصب والاحتيال عبر وسائل التواصل الاجتماعي.. كما أن هناك مجموعة من الجرائم التقليدية تُرتكب الآن عبر الفضاء السيبراني، ويشمل ذلك إنتاج وتوزيع المواد الإباحية للأطفال والأحداث ومؤامرات استغلالهم، والاحتيال المصرفي والمالي، وانتهاكات الملكية الفكرية، وجرائم أخرى، وكلها لها عواقب إنسانية

واقتصادية وقانونية كبيرة، وتتلخص أهميـة الأمـن السـيبراني، وإضـافة لـذلك تتلخص أهداف وجوده بما يأتي:

- توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها، وذلك بعدم السماح لغير المخولين بالوصول إليها باستخدامها.
- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكـف الأيـادي مـن العبث بها.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.
- حمايـة الأجهـزة والشـبكات ككّـل مـن الاختراقـات لتكـون درعٌ واقٍ للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدًا خلال العمل عبر الشبكة العنكبوتية.

والشكل رقم (1) يبين إحصائية صادرة عن المنتـدى الاقتصـادي العـالمي للعدد الإجمالي العالمي من حوادث الأمن الالكتروني بـالمليون خـلال الأعـوام (2009-2015م).



الشكل رقم (2) المصدر

https://www.weforum.org/agenda/2016/06/coulda-cyber-attack-cause-a-financial-crisis.

الفرع الثاني: فواعل الأمن السيبراني

من المهم التعرف على الفواعل الرئيسية في الأمن السيبراني، والتي تقسم إلى قسمين: الأول على المستوى الدولاتي، أمَا الثاني فهو على المستوى اللادولاتي، (لمين بلفرد، ص153)، ونشير إلى أن أستاذ العلوم السياسية الأمريكي جوزيف ناي من المفكرين الذين أشاروا لهذه الفواعل في دراسات له .

1- **الفواعل الدولاتية:**

بما أن الدولة هي الفاعل المحوري في تسيير الفضاء الافتراضي انطلاقاً من إمكاناتها المادية والبنيوية والبشرية والقانونية، نُشير هنا أساساً إلى الاحتكار القانوني والمُنظم للدولة للفضاء الافتراضي، من خلال مختلف أجهزتها.

2. **الفواعل اللادولاتية:**

ويتفرع في هذا القسم الدور المؤثر للأفراد والجماعات والمنظمات غير الحكومية والشركات، والذين أصبحوا في وقتنا هذا وبامتياز لديهم القدرة في التحكم في توجهات الدول وإدارتها وفق سياسات معينة من خلال الفضاء السيبراني، وتالياً أبرز الفواعل في هذا القسم:

- **الأفراد (Individuel):** حيث أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية والفضاء السيبراني، وله القدرة والإمكانية على إحداث الثورة الرقمية، وتُصبح هذه الثورة مجال استخدام للدولة نفسها، ومثال ذلك ما قام به المبرمج

الأمـريكي "مـارك زوكـربيرغ" (Mark Zoukerberg) في العـام 2004م، حين أَسَس مع زملاؤه شبكة (فـاس بـوك) لتسـتقطب أكـثر مـن مليـار مستخدم عبر العالم وتصبح أكبر موقع اجتماعي في العالم.

- **المنظمات غـير الحكوميـة (Nongovernmental Organizations):**

تعتبر هـذه المـنظمات شـبكة الانترنـت ووسـائل التكنولوجيـا الحديثـة عنصر أساسي في عملها مـن خـلال تعبئـة الـرأي العـام، والضـغط عـلى الحكومات مـن خـلال ترتيـب الحمـلات الاجتماعيـة وتعبئـة المجتمـع المدني للضغط على الحكومات للتغيير في سياسات معينة، والأمثلة عـلى ذلك كثرة مثل منظمات البيئة العالمية على اثـر قـرار الـرئيس الأمـريكي (دونالد ترامب) التخلي عن اتفاقيات التغير المناخي.

- **المجموعــات الافتراضــية (Default groups):** ونــذكر عــن تلــك المجموعات ما يقوم به القراصنة (Hackers)، حيث دائمـاً يسـعون إلى تحقيق أهداف مختلفة منها (السياسي، الربحي المادي، الأيـديولوجي)، أيضاً نجد المنظمات الإجرامية والتي تقوم هذه المـنظمات الإجراميـة بعمليات القرصنة السيبرانية، وسرقة المعلومات واخـتراق الحسـابات البنكيـة وتحويـل الأمـوال، كـما توجـد سـوق سـوداء عـلى الإنترنـت المظلم (Dark internet) لتجارة المخدرات والأسلحة والبشر.

- **الشركات المتعددة الجنسيات:** تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم شركات مثل: جوجل (Google) وفيسبوك (Facebook) ومايكروسوفت (Microsoft) ، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

- **الجماعات الإرهابية:** وهذه الفئة تعتبر من أبرز الفواعل الدولية، حيث أصبحت ومع تنامي ظاهرة الإرهاب تلجأ إلى الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال وغير ذلك، ومحاولة جمع المعلومات حول أهدافها، إضافة إلى التعامل مع الأسلحة المختلفة والتواصل مع عناصرها في أماكن ودول بعيدة، رغم أن هذه الجماعات لم تصل بعد إلى مرحلة القيام بهجمات سيبرانية حقيقية على منشآت البنية التحتية للدول.

المطلب الثالث

أبعاد الأمن السيبراني

إن ظهور الأمن السيبراني أدى وبشكل طبيعي إلى وجود انعكاسات وأبعاد لهذا المفهوم على البشرية؛ وسنتطرق إلى هذه الأبعاد مع شيء من الشرح وهي كالآتي:

- **الأبعاد العسكرية:**

لقد كانت نشأة شبكة الانترنت لأغراض ودواعي عسكرية في القرن الماضي، وتطورت فيما بعد لتشمل نواحي حياتية أخرى، ومن خلال قراءة التاريخ القريب نجد أن التنافس كان محموماً بين المعسكرين الشرقي والغربي ممثلاً بقطبيه الاتحاد السوفيتي، والولايات المتحدة الأميركية، في مجالات عديدة منها السباق على تطوير الأسلحة النووية من خلال الدراسات والأبحاث، أيضاً الوصول إلى الفضاء الخارجي، ومع تطور الوقت نجد أن دولاً عديدة في السنوات الأخيرة دخلت في هذا المجال، حيث منها من تعرض لهجمات سيبرانية واختراقات مختلفة، مثل ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، أيضاً تأزمت العلاقات بين دول مثال ذلك الذي حصل، بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في استونيا في العام 2007م، حيث دعا حينها وزير الدفاع (افيسكو) إلى اعتبار ذلك حرب عالمية ثالثة ودعوة الأمم المتحدة إلى

اتخـاذ إجـراءات لحمايـة الفضـاء الإلكـتروني. (عبدالصـادق، عـادل، 2009م، ص211).

وفي أيلول من العـام 2007م دعـا مجموعـة مـن الخـبراء الأمـريكيين في خطاب مفتوح إلى الرئيس الأمـيركي السـابق جـورج بـوش"، لتنبيهـه مـن خطـر الهجـمات السـيبرانية عـلى البنيـة التحتيـة الأميركيـة، التـي تضـم إلى الـدفاع، إمدادات الطاقة الكهربائية، والمياه، والاتصالات السلكية واللاسلكية، والخدمات الصحية، والنقل، والانترنت.

ومما يدل على أهمية البعد العسـكري للأمـن السـيبراني قيمـة الإنفـاق العسكري من قبل الدول في هذا المجال حيث بلغ الإنفاق العسكري على حرب الفضاء الإلكتروني (127) مليون دولار من أجمالي إنفـاق عسـكري بلـغ أربعـين بليون دولار في روسيا وتحتل روسيا المركز الرابع عالمياً في مجال تطـوير قـدرات الأسلحة الإلكترونية، بينما تـأتي الصـين في المركـز الثـاني عالميـاً في مجـال تطـوير قدرات حرب الفضاء الإلكتروني وتبلغ ميزانية الاتفاق عليهـا (55) مليـون دولار مـن إنفاقهـا العسـكري البـالغ (62) بليـون دولار، وهنـاك العديـد مـن الـدول تعكف على تطوير ترسانة الأسلحة الإلكترونية (عبد الصادق، مرجع سـابق، ص 208).

الأبعاد الاجتماعية:

إن ما يميز الشبكة العنكبوتيـة هـو أنهـا مفتوحـة المجـال للأفـراد يجولون فيها بأفكارهم وأرائهم المختلفة ومعلوماتهم في مجـالات عديـدة (فنية، علميـة، ....) في مجتمعـاتهم وذلـك عـبر صـفحات وغـرف دردشـة

ومدونات، وتعتبر هذه الآراء والمعلومات المختلفة، من الطرق التي تشكل رقي المجتمع وتطوره من خلال تبادل الأفكار والمعلومات بشكل ايجابي وخلاق، وسيلة لإغناء هذا المجتمع، وتطويره، بما تتيحه من فرص للاطلاع على الأفكار، والمعلومات، المختلفة، والفضاء السيبراني يضم مجتمعات لا تفصلها الحدود، تتبادل الخبرات والعلوم والمعارف مما يعزز أطر التعاون والتكامل بين المجتمعات البشرية.

وأصبحنا نشاهد ونلمس ما يقدمه الفضاء السيبراني من خدمات للإنسانية مثل التكافل الإنساني في حالات الكوارث الطبيعية، أو تبادل الخبرات الطبية التي يحتاجها فئات عديدة.

في هذا الصدد، تسعى جماعات مختلفة إلى تعزيز ونشر ثقافة الأمن في الفضاء السيبراني، وحث المجتمعات على ضرورة تعاون الأفراد بمختلف فئاتهم على تحقيق الأمن السيبراني بكافة جوانبه، لا سيما أن مخاطر الفضاء السيبراني تكاد تلمس جميع مكونات المجتمع، وذلك كون الخدمات والاحتياجات اليومية أصبحت مرتبطة بشكل أساسي على الفضاء السيبراني ومثال ذلك الطاقة، والنقل، والصحة، والاتصالات، وغيرها، ومن الطبيعي فالمجتمعات مدركة أن هنالك محتويات في الفضاء السيبراني تخالف الطبيعة البشرية السوية وأخلاقيات المجتمعات السليمة ومرفوضة فيها وهي بوجودها ستنعكس على هذه المجتمعات سلباً مما يؤدي إلى تفككها وتدميرها، ومن ذلك انتشار الجريمة وممارساتها، أما عن الأمور والمحتويات السلبية في الفضاء السيبراني والتي تهدد أمن المجتمعات: الإباحية، والترويج للاتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد

لقضايا تمس الأمن والسلام الدوليين. وتأسيساً عليه فالبعد الاجتماعي للفضاء السيبراني هو بعد مهم فالمجتمع الضعيف هو من أسباب ضعف الدولة وتراجعها، ولا بد من أن يكون المجتمع واعياً لمخاطر الفضاء السيبيراني، قادراً على التعامل ولو بشكل تأسيسي بسيط مع قواعد السلامة، ويدرك ما يترتب قانونياً عليه في حال تصرفاته التي تعرض أمن وسلامة الآخرين في المجتمع للخطر.

الأبعاد السياسية:

إن النظام السياسي في الدولة يسعى إلى المحافظة على كينونته واستقراره ومصالحه العليا، والمرتبط بالاستقرار الداخلي والسعي إلى رفاه مواطنيه، ومع التطور التكنولوجي والثورة الرقمية وظهور الفضاء السيبراني أصبح المواطن قادراً عن التعبير عن رأيه السياسي لا بل أصبح لاعب وطرف ومؤثر في السياسة الداخلية والخارجية للدولة، حيث ليس هنالك من صعوبة في الحصول على المعلومة ومعرفته بأمور بلده السياسية والقرارات المتخذة، كما أن الدول بالمقابل لم تتوانى في استثمار الفضاء السيبراني للوصول إلى أكبر نسبة من مواطنيها والتأثير عليهم ومحاورتهم، ومن جهة أخرى وكمثال حي استخدام الفضاء السيبراني للترويج للحملات الانتخابية للرؤساء وتقديم توجهاتهم وبرامجهم الانتخابية وأفكارهم السياسية وبطرق مختلفة.

الأبعاد الاقتصادية (جبور، منى الأشقر، الأمن السيبراني: التحديات ومستلزمات المواجهة، 2012م):

إن البعد الاقتصادي للأمن السيبراني هو ملازم له وبشكل لا يمكن إغفاله، بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، والمخزنة، والمستخدمة، على كل المستويات. كذلك، تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر إفادتها، من فرص الاستخدام، التي تقدمها الشركات الدولية، والشركات الكبرى، التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط. إلا أن هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة، والعمل، أو بحماية المستهلك على الانترنت.

يضاف إلى ذلك، دخول العالم، عصر المال الإلكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الالكترونية، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي. وتتنافس الشركات، على إصدار تطبيقات، تسمح بآليات دفع آمنة، وبحفظ المال في المحفظة الالكترونية، وبالإيفاء من خلالها، وباستخدامها كرصيد افتراضي. وقد وضعت بعض الدول تشريعات خاصة بهذا المال (Electronic money regulations, 2009). ونشير هنا إلى الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة وما ما يرافقها من صعوبات لمواجهتها منها الإجرائية ومنها التشريعية التي تسعى الدول إلى تطبيقها بالشكل المأمول.

الأبعاد القانونية:

إن الفضاء السيبراني ونشاط الأفراد والمؤسسات والشركات والحكومات في هذا العالم الإلكتروني، نتج عنه مستجدات قانونية وأوجب أن تكون هنالك قواعد قانونية جديدة تعمل على ترتيب هذا النشاط، وما رافقه من تحولات مثل الخصوصية وحق النفاذ إلى المعلومات، وكما ذكرنا في النقطة السابقة (البعد الاقتصادي)، أن هنالك انعكاسات اقتصادية، أيضاً تتطلب مستجدات في الجانب القانوني، ونؤكد أن البعد القانوني يتمحور، في حماية الأشخاص الطبيعيين والمعنويين، على السواء، وضرورة حماية البيانات، لاسيما الشخصية والحساسة منها، إضافة إلى حماية الحق في الخصوصية.

أما ومن جهة أخرى يضاف إلى هذا، ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية، والتجارية، على ضوء الحاجة إلى إعادة صياغتها، بما ينسجم مع توسع استخدام الشبكات الاجتماعية، والمسائل القانونية التي لا بد وأن تثار، على مستوى حماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال والمستخدمين، والملكية الفكرية. فالسنوات القادمة، لا بد وأن تشهد تصاعداً في إعداد، الأعمال الجرمية، والممارسات غير القانونية، التي تمارس في الفضاء السيبراني، ما يعني عملياً، ازدياد عدد القضايا التي سترفع أمام المحاكم، ما يستدعي، إعداد البيئة التنظيمية والتشريعية، وبناء قدرات هيئات المكافحة والحكم.

المبحث الثاني

من الجريمة السيبرانية إلى الإرهاب السيبراني

لا ينكر أحد أنه رغم الإيجابيات التي وفرتها الثورة التكنولوجية، إلا أن تلك الثورة رافقها تغيير وانعكاس في علم الجريمة , حيث أفرز الفضاء السيبراني أنواعاً جديدة من الجرائم ألا وهي الجرائم السيبرانية (cybercrimes)، وتعتبر هذه الجرائم بمختلف أنواعها رد فعل طبيعي ذلك كون الجريمة بشكل عام تتأثر بالمستجدات والتطورات التكنولوجية، وتعد هذه الجرائم موجهة إلى الأفراد والدول على حد سواء، والعنوان العريض لها هو الجرائم السيبرانية وتندرج تحت هذا العنوان أشكال عديدة، كما أن هذه الجرائم تختلف عن غيرها من الجرائم بعدد من الخصائص، حتى أن المجرم نفسه في هذا النوع من الجرائم يختلف عن المجرم التقليدي، أيضاً في الجانب القانوني. وبالنظر إلى كل من الجرائم السيبرانية والجرائم التقليدية نجد أن هنالك اختلافات بيتهما، وفي هذا المبحث سيتم التعرف على الجريمة السيبرانية من جوانب عدة.

المطلب الأول

الجريمة السيبرانية

ماهية الجرائم السيبرانية

تعددت التعاريف للجريمة السيبرانية وجاءت حسب اتجاهات ووجهات نظر مختلفة ومنها لفقهاء ومتخصصين وفي ما يلي أبرز ما جاء في تعريفها:

1- الفقيه الألماني تاديمان حيث عرفها: (هي كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي).

2- الفقيه الفرنسي (Masse) وعرفها : (الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح). (الشكري، عادل يوسف عبد النبي، 2008م. نقل بتصرف، ص 113.)

3- أما الفقيهين الفرنسيين (Le stanc, Vivant) بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".

4- بينما يعرفها الخبير القانوني جون فورستر بأنها: " كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"، ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسياً".

5- وقد عرفتها الدكتورة هدى حامد قشقوش في كتابها جرائم الحاسب الآلي في التشريع المقارن بأنها: " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات".

6- وعرفت منظمة التعاون الاقتصادي والتنمية (OCDE) الجريمة المعلوماتية في اجتماع باريس عام (1983م) بأنها: (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلَّق بالمعالجة الآليّة للبيانات أو نقلها) .

والجرائم السيبرانية لها مسميات عدة منها :

- جرائم الحاسوب والإنترنت.
- جرائم التقنية العالية.
- الجريمة الإلكترونية.
- الجريمة السايْبِريّة.
- جرائم أصحاب الياقات البيضاء.

أنواع الجرائم السيبرانية:

وبعد أن تعرفنا على تعريفات للجريمة السيبرانية، فلا بد أن نفرق بين أنواع الجريمة السيبرانية وأشكال الجريمة السيبرانية، وعليه نبدأ ونتعرف على أنواع الجرائم السيبرانية:

- **الجرائم ضد الأفراد:** أو ما يطلق عليه جرائم السايبر الشخصية وتتمثل في سرقة الهوية ومنها البريد الإلكتروني، أو سرقة الاشتراك في موقع شبكة الإنترنت وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت، بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل عملية الإجرام.
- **الجرائم ضد الملكية:** تتمثل في نقل برمجيات الضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، بهدف تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية.
- **الجرائم ضد الحكومات:** مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت، وهي تتركز على تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر وغالباً ما يكون هدفها سياسي.

أشكال الجرائم السيبرانية:

ويندرج تحت اسم الجرائم السيبرانية أشكال عديدة من الجرائم ولا بد من التعرف على هذه الأشكال وكما يلي:

1. **الجرائم التي تمس المعلومات الشخصية:** تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة

تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

2. **جرائم التعدي على البيانات المعلوماتية:** ويشمل هذا الشكل الجرائم التي يكون موضوعها البيانات المعلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرم اعتراض بيانات معلوماتية.

3. **جرائم التعدي على الأنظمة المعلوماتية:** تشمل هذه الجرائم ما يعرف بالولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ونتعرف على النظام المعلوماتي بحسب ما جاء في المادة الأولى من الاتفاقية الأوروبية - بودابست بأنه يتمثل: مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

4. **إساءة استعمال الأجهزة أو البرامج المعلوماتية:** تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازاً أو برنامجاً معلوماتيّاً أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقاً.

5. **جرائم تشفير المعلومات:** وتشمل حسب الإرشاد الخامس الصادر عن منظمة الاسكوا: أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة

في الدولـة، وأيضـاً بيـع أو تسـويق أو تـأخير وسـائل تشـفير ممنوعـة، (منظمة الإسكوا، الإرشاد الخامس، 2011م: 117).

6. **الجرائم الواقعة على الأموال بوسيلة معلوماتية:** تشمل جـرم الاحتيـال أو الغش بوسيلة معلوماتية، وجرم التزويد المعلوماتي، وجـرم الاخـتلاس أو سرقة أموال بوسيلة معلوماتية، وجرم أعمال التسويق والـترويج غـير المرغوب فيها، وجرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي، والاسـتخدام غـير المشروع لهـا، وجـرم الاطـلاع عـلى معلومات سرية أو حساسة أو إفشائها.

7. **جـرائم الاسـتغلال الجـنسي للقـاصرين:** تظهرهـا الأفعـال التـي تتعلـق باستغلال القاصرين في أعمال جنسية، وتشمل الرسـومات أو الصـور أو الكتابـات أو الأفـلام أو الإشـارات، أو أي أعـمال إباحيـة يشـارك فيهـا قاصرون، أو تتعلق باستغلال القاصرين في المواد الإباحية، وتشمل أيضاً إنتاج مـواد إباحيـة للقـاصرين بقصـد بثهـا بواسـطة نظـام معلومـاتي، وبالنظر إلى قانون الجرائم الإلكترونيـة الأردني رقـم (27) لعـام 2015م نجد في أن المادة التاسعة غطت ذلك **وكما يلي:**

أ- يعاقب كل من أرسل أو نشر عن طريـق نظـام معلومـات أو الشبكة المعلوماتية قصداً كـل مـا هـو مسـموع أو مقـروء أو مرئي، يتضمن أعمالا إباحية وتتعلق بالاسـتغلال الجـنسي لمـن لم يكمـل الثامنـة عشرة مـن العمـر بـالحبس مـدة لا تقـل

عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة آلاف دينار.

ب- يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسياً أو عقليّاً، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

ج- يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسياً أو عقليّاً، في الدعارة أو الأعمال الإباحية بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (15000) خمسة عشر ألف دينار.

8. **جرائم التعدي على الملكية الفكرية للأعمال الرقمية:** وحسب الإرشاد الخامس لمنظمة الاسكو تشمل الجرائم الآتية: جرم وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة (منظمة الأسكوا، الإرشاد الخامس للأسكوا، 2011م: ص109).

9. **جرائم البطاقات المصرفية والنقود الإلكترونية:** تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزويد نقود إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية، وعلى سبيل المثال ما جاء في المادة السادسة من قانون الجرائم الالكترونية رقم (27) لعام 2015م أنه يعاقب كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار، أيضاً أنظر المادة السابعة من نفس القانون.

10. **جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:** تشمل جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تحديد أشخاص أو التعدي عليهم بسبب انتمائهم العرقي أو المذهبي أو لونهم، وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

11. **جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:** تشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين، وجرم ترويج المواد المخدرة.

12. **الجرائم المعلوماتية ضد الدولة والسلامة العامة:** تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال معلوماتية، وتشمل أيضاً - جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، أنظر المادة الثانية عشر من قانون الجرائم الالكترونية الأردنية رقم (27) لعام 2015م.

وتسبب الجرائم السيبرانية بأشكالها التي ذكرناها خسائر اقتصادية كبيرة على الأفراد والمؤسسات والدول، هذا وتشير مجلة لوس انجلوس تايمز في عددها الصادر في 22 مارس عام 2000م إلى أن خسارة الشركات الأمريكية وحدها من جراء الممارسات التي تتعرض لها، والتي تندرج تحت بند الجريمة الإلكترونية بحوالي (10) مليار دولار سنوياً، وللتأكيد عل جانب قد تغفله الكثير من مؤسسات الأعمال، فإن نسبة (62%) من تلك الجرائم تحدث من خارج المؤسسة وعن طريق شبكة الإنترنت، بينما تشكل النسبة الباقية (38%) من تلك الخسائر من ممارسات تحدث من داخل المؤسسة ذاتها.

وفي ما يلي بعض الإحصائيات عن الجرائم السيبرانية الصادرة عام 2017م عن موقع (Symantec) ، وهي شركة عالمية تأسست في عام 1982م لبيع برامج الكمبيوتر وخصوصاً في مجال الأمن وإدارة المعلومات. يقع مقرها في كبيرتينو، كاليفورنيا، الولايات المتحدة الأمريكية (https://www.symantec.com/):

1. تضرر (978) مليون شخص في (20) بلداً بسبب الجريمة السيبرانية في عام 2017م.
2. تأثر (44%) من المستهلكين بجرائم الانترنت في الأشهر الـ (12) الماضية.
3. فقد المستهلكون الذين وقعوا ضحية للجريمة السيبرانية على مستوى العالم (172) مليار دولار، بمتوسط (142) دولاراً لكل ضحية.

أما أكثر الجرائم الإلكترونية شيوعاً:

(* 53%) وجود جهاز مصاب بفيروس أو تهديد أمني آخر.

(* 38%) الاحتيال على بطاقات الائتمان.

(* 34 %) اختراق الحسابات عن طريق سرقة كلمات المرور.

(* 34%) اختراق البريد الالكتروني أو حساب وسائل التواصل الاجتماعي.

(* 33%) الوقوع تحت عمليات الاحتيال عبر الإنترنت.

(* 32%) النقر على بريد الكتروني احتيالي أو تقديم معلومات حساسة (شخصية/ مالية) رداً على الاحتيال بالبريد الإلكتروني.

وقد بلغ عدد ضحايا الإنترنت عالمياً (968) مليوناً في أكثر من (20) دولة وفيما يلي عدد من الدول:

- الصين (353) مليوناً.
- الولايات المتحدة الأمريكية (144) مليوناً.
- المملكة المتحدة (17) مليوناً.
- كندا (10) ملايين.
- أستراليا (6) ملايين.
- البرازيل (62.21) مليوناً.
- فرنسا (19.31) مليوناً.
- ألمانيا (23.36) مليوناً.
- إندونيسيا (59.45) مليوناً.

خصائص وسمات الجرائم السيبرانية وما يميزها عن الجريمة التقليدية:

إن الجريمة السيبرانية تختلف وتتميز عن غيرها من أنماط الجرائم بعدة خصائص وسمات، منها الآتي:

1. إن الجريمة السيبرانية تتم في بيئة رقمية معلوماتية قوامها النظم المعلوماتية، وأجهزة ومعدات وأدوات وتجهيزات الحاسب الآلي، أي أنها تتبلور في المكونات المادية والبرمجية للحاسب الآلي.
2. الشخص الذي يقوم بفعل الجريمة له إمكانيات وطبائع تختلف عن غيره فهو محترف ولديه المعرفة والمعلومات وله صفاته فنية خاصة والعقلية ولا يشترط صفات بدنية معينة.
3. أن الأسلوب الجرمي في الجرائم السيبرانية لا يشترط فيه العنف، بل يتميز بالهدوء وضبط الأعصاب والنفس (المويشير، 200: 82؛ والغافري، 2011: 45).
4. من الصعب الحصول على الدليل الرقمي في الجريمة السيبرانية وسهولة وسرعة التخلص منها وإزالتها.
5. تتميز بأنها جرائم عابرة للحدود الوطنية واتصافها بالعالمية، كونها ليست مقتصرة على دولة واحدة بعينها، إذ يعتبر العالم مسرح للجريمة السيبرانية، وهنا المجرم السيبراني يستطيع ارتكاب الجريمة من بلد والضحية في بلد آخر (الغافري، 2011م: 5)
6. إن خاصية السرعة لهذه الجرائم هي ميزة لها حيث تتم الجريمة وتسبب الضرر في ثواني معدودة أو حتى أقل من ذلك.

7. تتم بالتعاون ما بين أكثر من شخص بأسلوب منظم أي بتعاون أكثر من شخص واحد في ارتكابها، إذ يشترك في إخراجها إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت تتوفر فيه الخبرة اللازمة التي تمكنه من تنفيذ جريمته، وشخص أخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراك سلبي، وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً إيجابياً وهو الغالب في الكثير من الجرائم ويتم في المساعدة الفنية أو المادية.
8. نسبة الخطر والضرر كبيراً في الجرائم السيبرانية لا سيما أنها أحياناً تستهدف أنظمة عسكرية وخدمات حيوية للدول مثل الكهرباء والمستشفيات وأمور مالية مثل البنوك والمصارف.
9. من ميزاتها تدني نسبة الإبلاغ عن تلك الجرائم من قبل المجني عليهم، سواءً كان المجني عليه شركة أو مؤسسة تجارية أو حتى فرد، ويعود السبب في ذلك بالنسبة إلى الأفراد الخوف على السمعة، أيضاً الشركات والمؤسسات فأنها تتجنب الإساءة لسمعتها ومما ينتج عنه من زعزعة ثقة العملاء في هذه المؤسسة.
10. الغموض، إذ يصعب إثباتها بدءاً من التحري والتحقيق وصولاً إلى المقاضاة والتي تواجه كل مرحلة صعوبات وتحديات معينة، أضف إلى أن الأساس أن المجرم هو مجهول الشخصية.

11. اعتبارها من الجرائم العابرة للحدود، وينتج عن ذلك بحد تحديات في الجوانب التحقيقية والقانونية والقضائية في الملاحقة والضبط والتفتيش. (صالح، 2006م: 7)

دوافع ارتكاب الجرائم السيبرانية:

لكل جريمة دافع ومن الصعب أن تجد جريمة بلا دافع، ويمكن تعريفه بأنه "هدف أو غاية مرجوة" تولد قناعة وإرادة لدى المجرم على ارتكاب فعل مجرم في القانون، وبعض خبراء القانون قالوا انه القوة المحركة للإرادة والعامل النفسي الذي يدعو إلى التفكير بالجريمة، والعزم على توجيه الإرادة إلى تنفيذها، وهنالك بعض التشريعات وبعض الأنظمة القانونية أطلقت عليه اسم "الباعث" وقد عرفه القانون الأردني رقم (16) لسنة 1960 في المادة (67) بأنه " هو العلة التي تحمل الفاعل على الفعل، أو الغاية القصوى التي يتوخاها". ولم يعتبره القانون في الفقرة الثانية من نفس المادة كعنصر من عناصر الجريمة إلا في الأحوال التي بينها القانون. وأن كان يدخل في تركيب الإرادة التي تشكل العنصر الأساسي والجوهري للقصد الجنائي "الركن المعنوي للجريمة"، والجرائم السيبرانية شأنها شأن غيرها من الجرائم ترتكب بدوافع متعددة ومتنوعة، نذكر أهمها الآتي:

- **الدوافع المادية:** تحقيق الكسب المادي والرغبة في تحقيق الثراء والتي تعتبر من الدوافع الرئيسية لارتكاب السيبرانية حيث يتم

اختيار المجني عليه في هذه الحالة بعناية بحيث يكون مقتدر مادياً.

- **الدوافع الشخصية، ومن صورها :**

- **الرغبة في التعلم وجمع المعلومات:** حيث يكرس مرتكبو هذه الجريمة وقتهم في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية سعياً منهم الاستيلاء على المعلومات.

- **دوافع ذهنية أو نمطية:** وتتم في رغبة المجرم السيبراني في قهر النظام الإلكتروني والتفوق على تعقيد الوسائل التقنية.

- **الانتقام:** وتتمثل في قيام شخص أو مجموعة من الأشخاص يمتلكون كم من المعلومات تخص المؤسسة أو الشركة التي يعملون بها تجعلهم يقدمون على ارتكاب جريمتهم.

- **التسلية:** كثير من الجرائم التي ترتكب من أجل التسلية ولا يقصد من ورائها أحداث جرائم.

- **الابتزاز والتهديد والتشهير:** حيث يكون القصد من وراء هذا الابتزاز أو التهديد أو التشهير في الأغلب هو الحصول على المال من المجني عليه مقابل التستر على خَطَإِ أو جعل الذي ارتكبه، ويكون انصياع المجني عليه للتهديد أو الابتزاز هو خوفه من فضه

أمره، وإطلاع الناس عليه، خاصة إذا كان المجني عليه له مكانة اجتماعية مرموقة.

- **الدوافع السياسية**: وتتمثل في تهديد الأمن القومي والعسكري، كحرب المعلومات والتجسس الإلكتروني والإرهاب الإلكتروني.

سمات المجرم السيبراني:

بعد أن تعرفنا على الجريمة السيبرانية وأشكالها وأنواعها لا بد أن نتعرف على المجرم السيبراني وبشكل واسع ومن أكثر من جانب، حيث تنوعت الدراسات التي تحدد المجرم، وتؤكد الدراسات أنه لا يمكن أن يكون هناك نموذج واحد للمجرم السيبراني، لكن هنالك سمات مشتركة بين هؤلاء المجرمين، ويمكن إجمالها في النقاط التالية:

✓ **التخصصية**: ذلك أن المجرم السيبراني يمتاز بمهارات يختص بها عن غيرته، وتكون هذه المهارات تقنية بحيث يستغل مداركه في فعل الجريمة، من خلال اختراق الشبكات وكسر كلمات المرور أو فك التشفير.

✓ **العود للإجرام**: حيث من صفات المجرم السيبراني أنه يعود للعمل الجرمي أكثر من مرة وبشكل شبه دائم، حيث يعود الكثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر، انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم، وأدت إلى تقديمهم إلى المحاكمة في المرة الأولى.

- ✓ **الاحترافية:** ذلك أن المجرم المعلوماتي له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهارات الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب (فريد، 2005م: 58).

- ✓ **الذكاء:** حيث أن الفضاء السيبراني بحر لا يستطيع الإبحار فيه إلا شخص يمتاز بالذكاء، كيف وإن كان هذا الشخص هو الذي يعرف مداخل ومخارج ونقاط الضعف والقوة في هذا الفضاء، إذاً فهو يمتلك من المعلومات ما يؤهله لأن يقوم بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب (فريد، 2005م: ص58).

- ✓ **الصبر:** إن تنفيذ الجرائم السيبرانية يحتاج أحياناً إلى وقت طويل من حيث الأعداد والتحضير، كما أن عمليات معينة تحتاج إلى خطوات مطولة، إضافة إلى أن المجرم السيبراني في حال فشله في تنفيذ مبتغاه يعاود مرة أخرى، وكل ما ذكرناه يحتاج إلى الصبر وهي من مزايا وخصائص المجرم السيبراني.

- ✓ **الهدوء:** والمقصود هنا أنه لا يشترط أن يكون المجرم هنا عنيفاً أو حتى يستعمل أسلوباً عنيفاً ودموياً لتنفيذ فعله، إذ أن هذا الجرم يحتاج إلى الهدوء أثناء التنفيذ، ولذلك دعا البعض إلى تسميتها جرائم (ذوي الياقات البيضاء).

فئات المجرمين السيبرانيين:

تعددت وجهات النظر والدراسات التي سعت إلى محاولة حصر أو تقسيم الجناة في الفضاء السيبراني إلى فئات، لكن مع اختلاف الآراء تكاد تكون متقاربة، وفيما يلي يرى المؤلف أن هذه الفئات فيها التقسيم المناسب للمجرمين السيبرانيين والتي حصرها في خمس فئات وكما يلي:

الأولى: العاملون على أجهزة الحاسبات الآلية بشكل شخصي في منازلهم؛ نظراً لسهولة اتصالهم بدون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

الثانية: الحاقدون: مثال ذلك في هذه الفئة الموظفون الساخطون على منظماتهم التي يعملون فيها فيبعدهم عن مقار عملهم بعد انتهاء مواعيد العمل يعملون على تخريب المواقع الخاصة بالمنظمة على شبكة الإنترنت أو إتلافها أو التشهير حتى بالمنظمة.

الثالثة: فئة المتسللين (Hackers) ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت. حالياً – تحت هذه الفئة بقسميها، ومن الأمثلة عن الأفعال التي ارتكبتها طائفة "الهاكرز" ما قامت به عصابة (414) الأمريكية والتي نسبت إليها أكثر من ستين (60) فعًلا وتعدى واختراقاً من خلال الحاسب الآلي مما نتج عنها أضرار بالمنشآت العامة والخاصة.

الرابعة: العاملون في الجريمة المنظمة، فمثلاً عصابات سرقة السيارات حيث يحددون بواسطة شبكة الإنترنت أسعار قطع الغيار المسروقة، ومن ثم يبيعونها في الأسواق الأعلى سعراً، أيضاً العاملون في الاتجار بالبشر، أو المروجون للمخدرات والممنوعات.

الخامسة: المجرمون المحترفون ويطلق على المجرمين المحترفين في الجريمة المعلوماتية الكراكرز (crackers) أو "الهاكرز" ذوي النوايا الآثمة، لذلك يجب التفرقة بين الصنفين "فالهاكرز" هو شخص متخصص أو خبير في إثبات الذات والجدارة، ويتمثل ذلك في دخولهم لقواعد مجال الحاسب الآلي ولديهم حب التحدي بالآخرين دون إلحاق الضرر بهم فقط بهدف التحدي، على خلاف "الكراكرز" فهو شخص متخصص أو خبير في مجال الحاسب الآلي، ولكنه يقوم بأنشطة غير قانونية تتمثل في تدمير الأنظمة المعلوماتية، فإن اعتداءاتهم تعكس ميولاً يظهر رغبتهم الإجرامية في إحداث إضرار بالغير.

أركان الجريمة السيبرانية:

يرى المؤلف أنه لا بد من التطرق إلى الجانب القانوني ولو بالشيء البسيط، وذلك ليكون هذا الكتاب قد غطى جميع جوانب الدراسة، والمقصود هنا بالجانب القانوني ليس الدولي إنما الجانب القانوني من حيث أركان الجريمة وحسب الترتيب الأتي:

أولاً: الركن المادي للجريمة

يمكن اختزال تعريف الركن المادي للجريمة بأنه الفعل أو النشاط الذي قام به الجاني لإبراز وإظهار الجريمة إلى حيز الوجود، حيث تبدأ الجريمة بفكرة إجرامية تعتمر في ذهن الجاني ثم تتطور وتكبر لتدخل في مرحلة العزم على تنفيذها، وهنا يبدأ العمل التحضيري المكون لهذا النشاط الجرمي والذي يدخل بعدها في مرحلة البدء بالتنفيذ دون العدول الاختياري عن تنفيذها.

أما النشاط أو السلوك المادي في جرائم الانترنت عامة والجريمة السيبرانية خاصة، فيتطلب الركن المادي فيها وجود بيئة رقمية مع الاتصال بالانترنت، وكذلك يتطلب معرفة بداية هذا النشاط والشروع فيه ونتيجته.

فالمجرم السيبراني يقوم بتحميل جهاز الحاسوب في المؤسسة المراد تهكيرها أو قرصنتها ببرامج اختراق أو فيروسات ضارة، لتحقيق الغاية الجرمية التي يسعى إليها، كما أن بعض جرائم الحاسوب لا تتطلب أعمال تحضيرية، مما يجعل هنالك صعوبة كبيرة في الفصل بين العمل التحضيري والبدء بالنشاط الإجرامي في الجرائم السيبرانية والجرائم المعلوماتية. إلا أن مجرد شراء برامج اختراق أو معدات الفك والتشفير وكلمات المرور يعد جريمة في مجال تكنولوجيا المعلومات.

عناصر الركن المادي للجريمة:

✓ **النشاط الجرمي:**

ويأتي هذا النشاط أما في شكل القيام بفعل يحضره المشرع الجنائي ويعاقب عليه أو الامتناع عن القيام بفعل رتب القانون على تركه وعدم القيام به جزاء أو عقوبة. وفي حال الامتناع عن القيام بالفعل تدخل هذه الحالة في نظام الجريمة التي ترتكب بسلوك سلبي وهو ما يعني أن يكون الإمساك عن فعل مطلوب القيام به قانونياً، مع الأخذ بعين الاعتبار أن كلا الفعلين يتركان أثراً واضحا في العالم الخارجي.

وهذا العنصر الأول من عناصر الركن المادي هو أساس الجريمة، حيث أن المشرع لا يعاقب على مجرد التفكير في الجريمة أو العزم على ارتكابها، إذا لم تترجم هذه النية أو العزم إلى أفعال مادية تدخل في تكوين الركن المادي لها، وبالتالي الدخول في مرحلة الشروع أو البدء بالتنفيذ لهذا النشاط الإجرامي.

✓ **النتيجة الجرمية:**

وهي الأثر الضار المرتكب أو الناتج عن النشاط الجرمي سواء كان هذا النشاط إيجابياً أو سلبياً، وتعتمد جسامة العقوبة على خطورة هذا النشاط الإجرامي، ومدى الأثر السلبي الذي يتركه في المحيط الخارجي حوله، فعلى سبيل المثال تختلف جسامة العقوبة بين النشاط الجرمي لمجرم الإيذاء البسيط عن العقوبة المقررة عن جرم الإيذاء البليغ، الذي يترك

ضرراً وأثراً كبيراً في المحيط الخارجي، لذلك تعتبر النتيجة الجرمية عنصراً هاماً وشرطاً أساسياً في تكوين الركن المادي للجريمة وفي حال حدوثها، فأنها تعطي صفة الكمال للنشاط الجرمي كنشاط مادي ملموس.

أما جرائم المعلوماتية والسيبرانية فأن النتيجة تواجه مشاكل عديدة، من حيث مكان وزمان تحقق النتيجة الإجرامية فيها، مثال ذلك قيام احد المجرمين السيبرانيين في الدولة (أ) باختراق جهاز الخادم (Server) لأحد البنوك في الدولة، (ب) وسرقة الأموال الموجودة فيه وهذا الخادم (Server) موجود في الدولة، (ج) فكيف يمكن تحديد ومعرفة وقت حدوث الجريمة، هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت بلد الخادم (Server)، وهنا تثور أيضاً إشكاليات القانون الواجب التطبيق وزيادة في هذه الإشكاليات، قد لا يكون هذا الفعل مجرماً في موطن أحد الأطراف مثلاً.

- ✓ **العلاقة السببية:**

وهي الارتباط السببي بين النشاط الجرمي والنتيجة الجرمية، لهذا النشاط، وهي شرطاً أساسياً للمساءلة الجنائية، حيث يكتمل الركن المادي بتوافرها، ولا يمكن تحقيق المساءلة الجنائية إلا بوجودها؛ فإسناد الفعل الجرمي إلى مرتكبه يتطلب وجود علاقة وثيقة بين الفعل وبين النتيجة، التي ترتبت على هذا النشاط الجرمي، وذلك لنفي أي لبس أو شائبة قد تحدث في حالة تعدد الجناة أو في حالة تعدد الجرائم.

- وعند البحث في العلاقة السببية نجد أن توافرها في العلاقة بين الفعل الجرمي والنتيجة يسهل على القاضي البت والحكم على هذا النشاط الجرمي، ولكن تثور الصعوبة في حال شابت هذه العلاقة، وجود سبب أو أسباب أخرى ساهمت في تحقيق النتيجة الإجرامية إلى جانب نشاط الجاني.

- وهنا فقد اخذ الفقه بثلاث نظريات في البت في هذا الموضوع وهي:

❖ **النظرية الأولى:** تسمى نظرية تكافؤ الأسباب وفحواها أن جميع الأسباب التي ساهمت في تحقيق النتيجة متساوية، من حيث القيمة القانونية بحيث يصلح كل سبب منها، لأن يكون وجوده سبباً في حدوث النتيجة، ومنطق هذه النظرية يقوم على التوسع في مجال المساءلة القانونية ومنعاً من الإفلات من العقاب.

❖ **النظرية الثانية:** تسمى نظرية السببية الملائمة وتقوم على الأخذ بالسبب الذي يصح اعتباره مؤدياً للنتيجة الجرمية حسب العادي والمألوف من الأمور، وهذا يتطلب من القاضي البحث في كل سبب على حده للوصول إلى السبب، الذي يمكنه أن يكون وفق المنطق العادي والمألوف سبباً في حدوث مثل هذه النتيجة.

❖ **النظرية الثالثة:** وهي نظرية السببية المباشرة، وتقوم هذه النظرية على اتصال السبب بالنتيجة الجرمية اتصالاً مباشراً دون أن يقطعهم سبب آخر، حتى يمكن مساءلة الجاني عن

جريمته التي ارتكبها، علماً أن البعض في الفقه الجنائي يطلق على هذه النظرية بالعلاقة المبنية على السبب الأقوى.

ثانياً: الركن المعنوي (القصد الجرمي):

وتعني العلم بعناصر الجريمة ويتكون هذا الركن من عنصري العلم والإرادة في التوجه إلى تحقيق الفعل والنتيجة الجرمية لهذا الفعل .

أما تحديد الركن المعنوي في الجرائم السيبرانية والجرائم المعلوماتية، فقد اختلف من نظام قضائي لآخر فتجد القضاء الأمريكي في تحديد الركن المعنوي، قد تنقل بين مبدأ الإرادة ومبدأ العلم فهو تارة يأخذ بالإرادة، كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحياناً أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي، كما تبنى أحياناً أخرى المعيارين معاً في قضية موريس، الذي كان متهما في قضية الدخول غير مصرح به على جهاز حاسب فيدرالي، فأخذت المحاكمة بمعيار الإرادة بالدخول غير المشروع به، وبمعيار العلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح، أما القضاء الفرنسي فأن منطق سوء النية هو الأعم في جرائم الانترنت، حيث يشترط المشرع للوصول إلى حالة التجريم إلى وجود سوء النية في النشاط الجرمي.

ثالثاً: الركن الشرعي (القانوني)

ويعني السند القانوني للتجريم سنداً للقاعدة القانونية الشرعية " لا عقوبة ولا جريمة إلا بنص " وهذا يضع حداً للاجتهاد القضائي في حال وجود النص الجزائي.

ونظراً لحداثة الجرائم السيبرانية ذات التقنية العالية، فقد تطلبت إيجاد نصوص قانونية تشريعية تحكمها. إلا إن هذا الأمر ليس بالأمر السهل، وبالرغم من ذلك فقد وضعت العديد من الدول تشريعات تنظم وتحكم هذا النوع من الجرائم نظراً لخطورتها، فقد قامت دولة السويد بإصدار قانون خاص بالجرائم المعلوماتية عام 1973م تحت مسمى قانون البينات ثم تبعتها بعد ذلك الولايات المتحدة الأمريكية، بإصدار قانون لحماية أنظمة الحاسب الآلي بين عامي (1976-1985م)، ثم تبعتها فرنسا في عام 1988م بتطوير قوانينها الجنائية لتتوافق مع ما استحدث من جرائم، وأما الدول العربية فقد قامت بعضها بسن بعض القوانين في مجال الجرائم الإلكترونية وبعضها لا زال بإجراءات سن قانون للجرائم السيبرانية كالأردن مثلاً، وسيتم التعرف على الجهود الوطنية من حيث سن وتشريع القوانين الوطنية، في تعزيز الأمن السيبراني في مطلب مستقل في الفصل الأخير من هذا الكتاب.

المطلب الثاني

الإرهاب السيبراني

يعتبر مصطلح الإرهاب قديم الاستخدام والنشأة، ولكن وفي العصر الحديث اختلفت صور الإرهاب، نظراً لما شهده العالم من متغيرات تكنولوجية، ويستخدم مصطلح الإرهاب للدلالة على إعمال العنف تهدف إلى إثارة الرعب في المجتمع الدولي أو الداخلي، ويعتبر تاريخ الحادي عشر من سبتمبر نقطة التحول العالمية الجديدة في مفهوم الإرهاب الدولي، وتزايد اهتمام الدول والمجتمع الدولي في مكافحة الأعمال الإرهابية، لا سيما في إطار منظمة الأمم المتحدة إلا أن هذا الاهتمام رافقه عدم اتفاق على تعريف مصطلح الإرهاب لسبب عدم توافر النية السياسية للتوصل إلى تعريف محدد للإرهاب من كافة الدول الأعضاء في المنظمة. (دولي، أحمد، **الإرهاب الدولي**، 2004م، ص30)

وبدراسة موضوع الإرهاب الدولي، يتبين أن هنالك علاقة وثيقة بين الإرهاب الدولي والهجمات الإلكترونية في الركن المعنوي، لهذه الجريمة ذلك أن القصد الجرمي لمنفذي الهجمات الإلكترونية يتقاربون مع منفذي العمليات الإرهابية التقليدية من حيث المضمون، حيث أن الهدف واحد وهو أثارة الرعب والخوف بين الآمنين من البشر، ولكن تختلف الوسيلة والطريقة ما بين حداثتها وخصائصها.

وفي هذا المطلب ستكون لنا وقفة مع الإرهاب الإلكتروني أو السيبراني بدءاً من المفهوم إلى الخصائص والأسباب وكما يلي:

ما هو الإرهاب السيبراني:

الإرهاب لغة: كما ذكرنا لم يتفق الفقهاء والسياسيين وذوي الاختصاص على تعريف جامع للإرهاب، وفي التعريف اللغوي للإرهاب ما يلي:

أولاً: تعريف الإرهاب لغةً

يجد المؤلف وبعد الرجوع إلى أمهات الكتب، والمتخصصة في اللغة العربية أن الأصل اللغوي لكلمة إرهاب، من الفعل "رهب" أي خاف، وأرهبه، واسترهبه، أي أخافه، والراهب هو المتعبد، ومصدره "الرهبة" و "الرهبانية" بفتح الراء و"التَرَهُب" هو التَعبُد (النقوزي، ص14)، وفي كتاب لسان العرب جاءت هذه الكلمة من (الرهبة، أي الخوف، أو هو التخويف، وإشاعة عدم الاطمئنان وبث الرعب والفزع (ابن منظور، لسان العرب، ص436).

وردت كلمة (رهب) في القرآن الكريم في العديد من السور ومنها قوله تعالى: ﴿ **يا بني إسرائيل اذكروا نعمتي التي أنعمت عليكم وأوفوا بعهدي أوف بعهدكم وإياي فارهبون**﴾ (سورة البقر، آية "40").

وعرف ابن منظور في كتابه لسان العرب في مادة (رهب): رهب بالكسر، يرهب رهبة ورهبا بالضم، ورهبا، أي خاف، ورهب الشيء رهبا ورهبة: خافه (أبو الفضل، ص437).

كما جاء استعمالها أيضاً بصيغة - استفعل من (استرهب) فلاناً أي رهبة وأفزعه وأخافه.

أما القرآن الكريم فقد جاءت مشتقات المصدر (رهب) في مواضع كثيرة، ودلالتها جاءت بمعنى (الخوف والفزع)، ولا ترتبط إطلاقاً القتال أو الحرب، حيث استعمل في كتاب الله الحكيم مصطلح (الرعب) للدلالة على القتال والحرب.

ثانياً: تعريف الإرهاب اصطلاحاً:

فيما يلي نذكر تعريف الأرهب اصطلاحاً بدءاً من ما جاء من تعريف في الموسوعات الاجتماعية والسياسية، حيث نجد الإرهاب قد تم تعريفه في أكثر من موسوعة ومن أبرزها:

- موسوعة علم العلاقات الدولية نجد أن الإرهاب يعني:

" أي نشاطات تقوم بها الدولة أو غير الدولة ويتم فيها استخدام العنف بقصد تحقيق أهداف سياسية محددة ". (خشيم، مصطفى، ط1، 1996: ص37).

- الموسوعة السياسية والعسكرية حددت سمات بأنها:

" عمل عنيف يُعرض الأرواح والممتلكات للخطر أو يهدد بتعريضها له، وهو موجه إلى أفراد أو مؤسسات أو مصالح تابعة لدولة ما ويقوم به أفراد (أو جماعات) مستقلون أو مدعومون من دولة ما، وقصده تحقيق أهداف سياسية". (البيطار، فراس، 2003: ص15-16).

- موسوعة العلوم الاجتماعية قد بينت كلمة الإرهاب أنه:

" نوع خاص من الاستبداد غير المقيد بقانون أو قاعدة، ولا يعبر اهتماماً لمسألة أمن ضحاياه، وهو يوجه ضرباته إلى أهدافه المقصودة بهدف خلق جو من الرعب والخوف، وشل فاعلية مقاومة الضحايا"، (David Roberson, 1985, p314).

- الموسوعة السياسية في تعريفها للإرهاب بأنه:

" الإرهاب هو استعمال العنف غير القانوني، أو التهديد به بأشكاله المختلفة، كالاغتيال والتشويه والتعذيب، والتخريب والنسف، بغية تحقيق هدف سياسي معين، مثل كسر روح المقاومة والالتزام عند الأفراد، وهدم المعنويات عند الهيئات والمؤسسات، كوسيلة من وسائل الحصول على المعلومات أو المال، وبشكل عام استخدام الإكراه لإخضاع طرف مناوئ لمشية الجهة الإرهابية " (الكيالي، عبد الوهاب، 1985: ص153).

أما التعريفات للفقهاء والمختصين من أبرز هذه التعريفات ما يلي (زرقط، عمر، 2017: ص27):

- يعرفه "سوتيل" الإرهاب أنه: "العمل الإجرامي المصحوب بالرعب أو العنف أو الفزع بقصد تحقيق هدف محدد".

- ويعرفه "ليمكين" الإرهاب بنظرة عامة بأن قال أنه: "يقوم على تخويف الناس بمساهمة أعمال العنف".

- كما أشار الفقيه " والتر" ، إلى تعريف العمل الإرهابي أو الإرهاب بأنه: "عملية إرعاب تتألف من ثلاث عناصر: فعل العنف أو التهديد باستخدامه وردة الفعل العاطفية الناجمة عن أقصى درجات خوف الضحايا أو الضحايا لمحتملين، والتأثيرات التي تصيب المجتمع بسبب العنف أو التهديد باستخدامه والخوف الناتج عن ذلك ". (الحلو، حسن، 2007: ص38)

- وعرفه المفكر الوازي، بأنه: "بمثابة فعل يرمي إلى قلب الأوضاع القانونية والاقتصادية التي تقوم على أسسها الدولة". (حومد، 1964: ص220).

- ويعرفه شميد بأنه: "الإرهاب هو أسلوب من أساليب الصراع الذي تقع فيه الضحايا جزافاً كهدف عنف فعال وتشترك هذه الضحايا الفعالة مع جماعة أو طبقة في خصائصها مما يشكل أساسا لانتقائها من أجل التضحية بها. (مولود، رنا، 2011: ص160).

- وعرفه نومي غال بأنه: "طريق عنيفة أو أسلوب عنيف للمعارضة السياسية، وهو يتكون من العنف والتهديد به، وقد يتضمن التهديد أو العنف البدني الحقيقي، أو ممارسة العنف النفسي، وقد يمارس

الإرهاب ضد أبرياء، أو ضد أهداف لها ارتباط مباشر بالقضية التي يعمل الإرهابيون من أجلها". (Noemi Gal, 1985: p2).

وكانت هنالك جهود لمفكرين عرب في محاولات لوضع تعريف للإرهاب، ومن نتاج هذه الجهود التعريفات الآتية:

- عرف أسامة الغزالي الإرهاب على أنه: " هو فعل أو أفعال العنف البدني الذي يستهدف إيذاء الكيان الإنساني جسدياً إلى حد القتل، وينطوي ذا الفعل على انتهاك عمدي للقواعد الأخلاقية والعرفية والقانونية للسلوك الإنساني بغرض بث الشعور بالخوف وعدم الأمن ويتصف هذا الفعل بالطابع الرمزي، بمعنى أن يحمل رسالة ما إلى كافة الضحايا المحتملين الآخرين ليزرع الرعب في قلوبهم ويستهدف هذا الفعل التأثير على السلوك السياسي للدولة أو للدول التي ينتمي إليها الضحايا". (معوض، جلال، 1987: ص171).

- وفي تعريف صلاح الدين عامر، للإرهاب أنه: " الاستخدام المنظم للعنف لتحقيق هدف سياسي، وبصفة خاصة مجموعة أعمال العنف التي تقوم منظمة بممارستها على المواطنين لخلق جو من عدم الأمن، كأخذ الرهائن واختطاف الأشخاص ووضع المتفجرات أو العبوات الناسفة في أماكن تجمع المدنيين أو وسائل النقل العامة والتخريب " (صلاح الدين، عامر، 1977: ص4).

ثالثاً: تعريف الإرهاب في المواثيق الدولية

جاءت هنالك اتفاقيات دولية عديدة في تعريف الإرهاب ونضع هنا عدداً من هذه التعاريف:

- الإرهاب: الأعمال الإجرامية الموجهة ضد دولة ما بغرض إثارة الفزع والرعب لدى شخصيات معينة أو جماعة معينة أو جماعات من الناس أو لدى الجمهور. (الفقرة الثانية من المادة الأولى من اتفاقية جنيف لعام 1937م لمنع وقمع الإرهاب لدولي المنعقدة في 1937/11/16م).
- إن أول اتفاقية عربية وضعت تعريفاً للإرهاب، وبينت آلية التعاون العربي بشكل جماعي لمكافحة الإرهاب، هي اتفاقية التعاون العربي لمكافحة الإرهاب لعام 1998م وعرفت الإرهاب أنه " كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروع إجرامي فردياً أو جماعياً، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر"، وفي تعريف الجريمة الإرهابية بينت الفقرة الثانية من المادة الأولى التعريف الآتي: "أي جريمة أو شروع فيها ترتكب تنفيذاً لغرض إرهابي في أي من الدول المتعاقدة أو على رعاياها أو على ممتلكاتها أو مصالحها يعاقب عليها قانونها الداخلي".

- في عام 2004م تم إعداد تقرير من قبل عدد من الخبراء من ذوي الاختصاص في مجال مكافحة الإرهاب وكان عنوان تقريرهم المقدم إلى الأمين العام " عالم أكثر أمناً، ومسؤوليتنا المشتركة "، حيث اقترح الخبراء تعريف الإرهاب بأنه: "أي عمل يقصد به التسبب في الوفاة أو الأذى البدني الجسيم بالمدنيين أو غير المقاتلين حينما يكون الغرض من مثل هذا العمل بحكم طبيعته أو سياقه هو تخويف السكان أو إجبار الحكومة أو منظمة دولية على تنفيذ أي فعل أو الإحجام عن تنفيذه". وهذا التعريف هو إلى حد كبير نفس الذي اقترحه مجلس الأمن الدولي، ولكنه يضيف مفهومي المدنيين أو "غير المقاتلين" كهدفين محتملين للهجمات الإرهابية. (قرارات هيئة الأمم المتحدة).

بعد أن تعرفنا على ما جاء من تعريفات للإرهاب ننتقل إلى الإرهاب السيبراني وشأنه شأن تعريف الإرهاب منفرداً، حيث لا يوجد اتفاق على هذا التعريف، وقد كانت بداية استخدام مصطلح الإرهاب الإلكتروني (Cyberterrorism) في الثمانيات من القرن العشرين على يد باري كولين (Barry Collin)، والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب التكنولوجي. ولكنه تبنى تعريفاً للإرهاب الإلكتروني مقتضاه؛ بأنه "هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب". (عبد الصادق، عادل، مرجع سابق، ص 104)

ويعرفه دورثي دينينغ (Dorothy Denningg) هو "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب" (DOROTHY E. DENNING, 2000, p1).

كما نجد أن جيمس لويس (James Lewiss) وضع تعريفاً قريباً للسابق وعلى أنه: "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين". (.Alix DESFORGES, quel périmètre, 2011, p.03).

وتعرفه وكالة المخابرات المركزية الأمريكية: الإرهاب الالكتروني هو أي هجوم تحضيري ذي دوافع سياسية موجه ضد نظم معلومات الكمبيوتر وبرامجه والبيانات والمعلومات التي تنتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين.

وتضع وزارة الدفاع الأمريكية التعريف التالي: أنه عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث أو بث الخوف تجاه متلقي الخدمات مما يسبك الارتباك وعدم اليقين، وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة.

خصائص وسمات الإرهاب السيبراني:

هنالك عدد من الخصائص والسمات للإرهاب السيبراني والتي بنفس الوقت تعتبر سمات تحفز الجماعات الإرهابية المتطرفة على توظيف هذا الفضاء واستخدامه لغايات إرهابية عنيفة وكما يلي:

- **انخفاض التكلفة:** مقارنة بالإرهاب التقليدي يعتبر الإرهاب السيبراني أقل كلفة تكلفة بالنسبة للجماعات الإرهابية والمتطرفة، ذلك أن الإرهاب السيبراني لا يتطلب شراء الأسلحة والمتفجرات والمعدات، أضف إلى ذلك تكاليف السفر وتدريب العناصر والتخطيط، بحيث تقتصر تنفيذ العمليات الإرهابية السيبرانية على أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت والمهارات التقنية اللازمة، كما أنها لا تحتاج إلى عناصر بشرية كبيرة أو حتى جهداً جسدياً، وفي حال الصدام لن تخسر هذه الجهات خسائر بشرية وهي أمور جاذبة للجماعات الإرهابية المتطرفة.

- **مجهولة المصدر:** إن هوية الإرهابي من الصعوبة التعرف عليها في الفضاء السيبراني، وذلك لأسباب وعوامل كثيرة من أبرزها:

  - وجود طرق ووسائل تقنية حديثة تساعد على إخفاء هوية الإرهابي على الإنترنت؛ حيث يقوم المجرم مثلاً بتغيير عنوان بروتوكول الإنترنت (IP) - الذي يمكن استخدامه لتتبع مجرمي الإنترنت- عبر أجهزة الكمبيوتر المخترقة إلى مستخدمين أبرياء.

- استخدام أسماء مستعارة من قبل هذا الشخص المجرم، وتسجيل الدخول إلى مواقع الويب المختلفة بهوية مجهولة بقصد إخفاء هويتهم الحقيقية، مما يسبب صعوبة من قبل أجهزة الدولة على تعقبهم وتحديدهم.
- في الفضاء السيبراني عكس الواقع على الأرض، حيث تكون مواجهة الجماعات الإرهابية بأساليب مادية مختلفة، أما الفضاء السيبراني لا توجد هذه الأدوات المادية التي تواجه التنظيمات الإرهابية، مثل: السيطرة على الحدود بين الدول، ووجود نقاط التفتيش، والأجهزة التي تكشف المواد الممنوعة، وغير ذلك.

– **سرعة تنفيذ الفعل الإرهابي وبوقت قصير:** إذ يمكن إطلاق برامج ضارة مثل فيروسات الكمبيوتر والديدان وبثها خلال فترة زمنية قصيرة للغاية دون أدنى تدخلٍ بشري, ولا بد من الإشارة إلى نقطة مهمة ألا وهي إن السرعة التي تنتشر بها تلك البرامج الضارة لا تتصل بالشخص المهاجم، بل بسرعة اتصال الضحايا بالإنترنت.

تنوع الخيارات المستهدفة (تعدد الأهداف المحتملة): وهنا يكون المجال والخيارات متاحة للمهاجم السيبراني (الإرهابي)، حيث الأهداف المحتملة ما بين أجهزة وشبكات الكمبيوتر الخاصة بالحكومات، والأفراد، والمرافق العامة، وشركات الطيران الخاصة، وغير ذلك، وهذا الأمر يزيد من خطورة استهداف البنى التحتية الحيوية للدولة، مثل: شبكات الطاقة الكهربائية، والمرافق الخدمية

مثل الطوارئ نظراً أن هذه البنى تعتمد على أنظمة كمبيوتر في ديمومتها وتشغيلها.

- **عدم التقيد بالنطاق الجغرافي:** وهنا نجد أن الهجمات السيبرانية عند تنفيذها ليس بالضرورة أن يكون الإرهابي في نفس الموقع والمكان، أو يكون مراقباً بشكل مباشر أو يتم اعتقاله في حينها وفعله الإرهابي يكون موجه من مكان بعيد وأحياناً خارج حدود الدولة المستهدفة، وحتى يصل الأمر أن يكون في قارة أخرى.

وسائل الإرهاب السيبراني:

تتعدد الوسائل التي يستخدمها الإرهابيون في تنفيذ هجماتهم من خلال الفضاء السيبراني ومن أبرز تلك الطرق والوسائل:

- **البريد الإلكتروني:** البريد الإلكتروني هو الوسيلة الأولى من وسائل يستخدمها الإرهابيون حيث يستغلون هذه الخدمة في التواصل فيما بينهم ، بسرعة ودون رقابة واختلاف المكان بين المرسل والمستقبل .

- **إنشاء مواقع الانترنت:** يعرفها موقع ويكيبيديا الموسوعة الحرة "هي مجموعة صفحات ويب مرتبطة مع بعضها البعض، ومخزنة على نفس الخادم. يمكن زيارة مواقع الويب عبر الإنترنت.. تختلف أهداف مواقع الويب، فمنها ما هو للإعلان عن المنتجات ومنها ما يبيعها، كما أن هناك مواقع للمحادثة (الدردشة) أو منتديات للنقاش

والحديث بين مستخدمي الويب. ويوجد ما يعرف بالمدونات وهي مواقع ويب يسرد فيها مؤلفها ما يريد الكتابة عنه ومواضيع أخرى, كما يمكن للزوار الرد على ما يكتب".

فالمواقع الإلكترونية من خلال التعريف السابق بيئة خصبة للمنظمات الإرهابية لأنشطتهم من خلال تبادل الآراء والأفكار، حيث فيها يلتقي عدد كبير من الأشخاص بدون قيود في موقع افتراضي واحد وفي نفس الوقت مما يسهل في نشر الأفكار وحتى الإشاعات والمبادئ من خلال الحوار.

- **اختراق وتدمير المواقع:** تتم عملية الاختراق الإلكتروني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي. أما تدمير المواقع فهو الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (PC-Server) أو مجموعة نظم مترابطة شبكيًا (Intranet) بهدف تخريب نقطة الاتصال أو النظام. (السند، عبد الرحمن بن عبد الله، وسائل الإرهاب الإلكتروني، الموقع الإلكتروني)

ومـن الأمثلـة عـلى اختـراق وتـدمير المواقـع الإلكترونيـة قيـام الإرهابيين باختراق صفحة إلكترونية لمستشفى وتهديد حياة المرضى فيه عن طريق التلاعب بأنظمة العلاج، أو تهديـد الاقتصـاد لدولـة مـا مـن خلال اقتحام مواقع البورصة فيها، أو حتى اختراق برامج الاتصـالات في المطارات والجامعات، أيضاً الاختراق والتعطيـل إلى الأنظمـة الأمنيـة في دولة معينة لصالح الجماعة المتطرفة.

أنواع الإرهاب السيبراني:

هنالك نوعان من الإرهاب؛ يشير أولهما إلى الإرهـاب السـيبراني النقـي (Pure Cyber Terrorism)، بينما يُشير الثـاني إلى الإرهـاب السـيبراني الهجـين (Hybrid Cyber Terrorism).، وفيما يلي نظرة إلى كل منهما:

أولاً: الإرهاب السيبراني النقي

يـرتبط الإرهـاب السـيبراني الخـالص بـالهجوم مبـاشر عـلى البنيـة التحتية الإلكترونية والشبكات الاجتماعية والمعلومات المخزنة فيها لأغراض سياسية واجتماعية، ويمكن أن يتفرع هذا النوع من الإرهاب إلى فـرعين؛ الأول يستهدف التلاعب وإفسـاد وظـائف أنظمـة المعلومـات وإتـلاف أو تـدمير الأصـول الافتراضـية والماديـة، باسـتخدام فيروسـات الكمبيـوتر، والديدان، وأحصنة طـروادة، وهجـمات الفديـة. أمـا الفـرع الثـاني يـرتبط بالقرصـنة المصـممة لهـدم المواقـع الإلكترونيـة، وتعطيـل الحيـاة اليوميـة

باستهداف البنية التحتية التي تدار بأجهزة الكمبيوتر، مثل المستشفيات، والمطارات والبورصة... الخ.

ثانياً: الإرهاب السيبراني الهجين

إن الفضاء السيبراني أتاح للجماعات المتطرفة استخدام هذا المجال وتوظيفه لخدمتهم وأعمالهم العنيفة والمرفوضة، من خلال نشاطات مختلفة وهو ما يندرج تحت هذا النوع (الهجين) وفيما يلي أبرز الأنشطة المستخدمة:

- **نشر الأفكار المتطرفة (الدعاية والإعلان):** تستغل الجماعات الإرهابية الفضاء السيبراني في جانب الدعاية والإعلان من خلال قيامها بنشر الأفكار المتطرفة عبر وسائل التواصل الاجتماعي مثل غرف الدردشة والتي يجتمع فيها جميع شرائح المجتمع وخصوصاً الشباب منهم، أضف إلى ذلك وجود مواقع وصفحات الكترونية تعود للجماعات الإرهابية، وفي تقرير للخبير الأمني في قضايا الإرهاب الرقمي جيف باردين كشف أن التنظيم الإرهابي لداعش لديه (90) ألف صفحة باللغة العربية على موقع التواصل الاجتماعي الفايسبوك و (40) ألف بلغات أخرى، إضافة إلى موقعه الذي دشنه التنظيم بسبعة لغات لابتزاز الشباب وضمهم لصفوفهم فحوالي (3400) شاب انضم إلى داعش عن طريق حملات التنظيم الالكترونية. فحسب جمعية آفاق للأمن الداخلي لتونس أن المواقع الإلكترونية ذات التوجه المتطرف والإرهابي تستقطب نحو ألف شاب في السنة وهو يعادل (3) شبان يومياً، وهو رقم مرتفع يعكس

خطورة الظاهرة التي تزداد حدتها وهم يمثلون حوالي (40%) من مجموع الشباب المستقطب وهم من الطلبة والتلاميذ المتفوقين الذين تتراوح أعمارهم بين (17 و 28) سنة والذين يدرسون الاختصاصات العلمية الطب، الفيزياء والكيمياء، حيث تقوم هذه الجماعات باستثمار مهاراتهم العلمية لأغراض تخريبية.

- **التنسيق و التواصل الآمن:** من الطرق التي تستخدمها الجماعات الإرهابية للتواصل فيما بينها وسائل التواصل الاجتماعي وذلك من خلال غرف دردشة الألعاب وتطبيقات الرسائل المشفرة مثل (Kik - SuperSpot - Wickr - Gajim)، ويكون التواصل العابر للحدود والسريع ومحدودية الرقابة وإخفاء المعلومات الشخصية لأطراف الاتصال.

- **التجنيد الالكتروني:** أصبح التجنيد الإلكتروني للجماعات الإرهابية طريقة حققت معها هذه الجماعات المتطرفة إضافة عناصر جدد ومن دول وجنسيات مختلفة وبأعداد ليست بالقليلة، ويتم ذلك من خلال تحديد المجندين المحتملين من خلال مراقبة ملفات التعريف والمحادثات على تلك المواقع، والتي من خلالها يتبين مدى تعاطفهم وقبولهم للفكر الإرهابي، حيث تتم عملية التجنيد بطرق ومراحل مختلفة وذكية أوقعت العديد من الشباب في براثن هذه الجماعات المتطرفة الشريرة.

- **التـدريب:** تقـوم الجماعـات الإرهابيـة باسـتخدام الفضـاء السـيبراني والتواصل مع عناصرها وتدريبهم عن بعد عـلى كيفيـة شـن الهجـمات وتصنيع المتفجرات وتحميل الفيديوهات التي توضح ذلك.

وعلى الصعيد الإلكـتروني مثـال الاسـتخدام المتطـور للجماعـات الإرهابية ما جـاء في "دليـل تـدريب القاعـدة (Al-Qaida Training Manual) عـلى سـبيل المثـال. فقـد شـمل الـدليل إرشـاداتٍ حـول الاسـتخدام الصـحيح للاتصـالات وحمايـة البيانـات. كـما يشـير الـدرس الثالث عشر من الدليل إلى الكتابـة السريـة والأصـفار والرمـوز، بهـدف تدريب الأعضاء المحتملين على نقل البيانات بشكلٍ آمن. إذ يتم تشـفير التعلـيمات الحاليـة والمسـتقبلية دون أن تتضـمن التوقيتـات والمواقـع المستهدفة، وهو ما ينطبق بالمثل عـلى وثـائق تنظـيم "القاعـدة" التـي تزيد على (100) وثيقة، لإخفاء أدلة ومـواد التـدريب. (البهـي، رغـدة، الإرهاب السيبراني، انظر الموقع الإلكتروني).

- **جمع التبرعات (التمويل الإلكتروني):** اسـتخدمت أفـراد الجماعـات الإرهابية القنوات الإلكترونية كمنفذ لتمويل عملياتها واتخذت مـن العمل الخيري غطاءً لجمع الأموال ودعم مشاريعها المدمرة، وهـذه أحد صور الإرهاب السيبراني، حيث إن هـذه الجماعـات تحتـاج إلى المال لدعم أعمالها والتزود بالسلاح وتجد مـن جمـع التبرعـات عـبر الإنترنت ووسائل التقنية طريقاً لنيل مرادهـا. إن محاربـة الإرهـاب الإلكتروني لا تقع عـلى عـاتق الـدول فقـط وإنمـا عـلى عـاتق الفـرد

أيضاً، وحسب تقرير أحد الصحف البريطانية فقد بلغت الأموال بحوزة جماعات تنظيم الدولة "داعش" ما يزيد عن (2) بليون دولار، مما يمدهم بالقدرة القتالية على المدى البعيد. ومن أبرز مصادر التمويل لهذه الجماعات هو استخدام وسائل التقنية والإنترنت، والتي عن طريقها يمكنهم سرقة الهوية، بطاقات الائتمان، المزاد الوهمي، الاحتيال بالأسهم، وجمع التبرعات (المركز الدولي للأبحاث والدراسات).

- **جمع المعلومات** أصبحت معلومات الأفراد الشخصية والمعلومات عن المواقع والمنشآت، وبسبب عدم أخذ الاحتياطات اللازمة لأمن الحسابات الشخصية، حيث يستغل الإرهابيون الفضاء السيبراني من خلال ذلك لجمع معلومات عن الأهداف المحتملة، إضافة إلى ذلك من الأمثلة المعلومات المتصلة بالبيانات الشخصية للأفراد مثل مكان السكن والعمل وغير ذلك، إضافة إلى الأماكن التي يترددون عليها.

الفصل الثاني

الجهود الدولية والوطنية في تعزيز الأمن السيبراني

المبحث الأول

واقع الأمن السيبراني دولياً وعربياً (مؤشرات وأرقام)

(2017-2108م)

تبذل الدول على مستوى العالم جهوداً تنفيذية وتشريعية لتعزيز أمنها السيبراني، وهنالك مؤسسات دولية متخصصة في هذا الشأن ساعد وجودها على قياس مدى التزام الدول في تعزيز الأمن السيبراني، وتعتبر هذه المؤسسات بوجودها مصدر معلومات يستفيد منه كل من الدول والمتخصصين والباحثين، وللتعرف إلى واقع الأمن السيبراني في دول العالم بشكل عام والدول العربية بشكل خاص لا بد من الاستناد إلى أرقام وإحصائيات ومؤشرات موثوقة المصدر، وسيتم التعرف على هذا الواقع بالاستناد والاستئناس إلى تقارير الاتحاد الدولي للاتصالات التابع للأمم المتحدة (ICT) للأعوام 2017م 2018م بنسختيه الثانية والثالثة من التقرير العالمي للأمن السيبراني .

والاتحاد الدولي للاتصالات وهو وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT) ، أُنشئ الاتحاد في عام 1865م في باريس تحت اسم الاتحاد الدولي للبرق، ويرجع اسمه الحالي إلى عام 1934م، وفى عام 1947م، أصبح وكالة متخصصة تابعة للأمم المتحدة، يأتي عمل الاتحاد الدولي للاتصالات في صميم قطاع تكنولوجيا المعلومات والاتصالات، إذ يؤدي دور الوسيط لتيسير الاتفاق

على التكنولوجيات، وتوزيع الموارد العالمية مثل طيف التردد الراديوي والمواقع المدارية الساتلية، بغية استحداث نظام عالمي سلس للاتصالات يتسم بالقوة والثقة والتطور المستمر.

يقوم الاتحاد الدولي للاتصالات منذ نشأته على الشراكة بين القطاعين العام والخاص، ويبلغ عدد الأعضاء فيه حالياً (193) بلداً، وما يزيد على (800) كيان من كيانات القطاع الخاص والمؤسسات الأكاديمية، ويقع مقره في جنيف، سويسرا، ويضم (12) مكتباً من المكاتب الإقليمية ومكاتب المناطق في جميع أنحاء العالم، ويشمل أعضاء الاتحاد مجموعة واسعة من قطاع تكنولوجيا المعلومات والاتصالات في العالم، من أكبر شركات التصنيع وشركات التشغيل إلى الأطراف الفاعلة الصغيرة المبتكرة، التي تستعمل تكنولوجيات جديدة أو ناشئة إلى جانب مؤسسات البحوث والتطوير الرائدة والدوائر الأكاديمية.

ويقوم الاتحاد بقياس مدى التزام البلدان في مجال الأمن السيبراني كل عامين وتقييم كل دولة بناء على خمس ركائز - (1) التدابير القانونية، (2) التدابير الفنية، (3) التدابير التنظيمية، (4) بناء القدرات (5) التعاون - ثم تجميعها في النتيجة الإجمالية:

أولاً: العام 2017م

أصدرت وكالة الأمم المتحدة للاتصالات النسخة الثانية من المؤشر العالمي للأمن السيبراني (GCI) في العام 2017م، وأبرز ما جاء فيه من تصريحات:

- بينت الوكالة أن الحاجة تدعو إلى بذل مزيد من الجهد في هذا المجال الحرج، خاصة أن الحكومات تعتبر المخاطر الرقمية ذات أولوية عالية، وقد أصبح الأمن السيبراني مصدر قلق كبير للدفاع القومي.
- أظهرت الدراسة وجود فجوات كبيرة في الأمن السيبراني بين الدول الأكثر قوة في العالم.
- امتلاك حوالي نصف جميع البلدان استراتيجية للأمن السيبراني أو أنها بصدد وضع استراتيجية.
- حثت المزيد من البلدان على النظر في السياسات الوطنية للحماية من الجرائم السيبرانية.
- الهجمات الإلكترونية تزداد تعقيداً وقادرة على الوصول إلى شبكات الكهرباء وإغلاق المستشفيات وسرقة الشركات.

أما عن مؤشرات وترتيب الدول إن أبرز ما جاء في التقرير ما يلي:

- نحو (38) في المئة من البلدان لديها استراتيجية منشورة للأمن السيبراني، (12) في المئة من الحكومات الأخرى بصدد وضع استراتيجية واحدة.
- حصلت سنغافورة على أعلى تصنيف من حيث الأكثر التزاماً.

- جاءت الولايات المتحدة التي جاءت في المركز الثاني.

- تفوقت الولايات المتحدة على سنغافورة من حيث العوامل القانونية والتنظيمية والنمو المحتمل، وسجلت سنغافورة أعلى علامة من حيث التعاون.

- باقي الدول الـ (10) الأكثر التزاماً في مجال الأمن السيبراني وهي على التوالي ماليزيا وعمان واستونيا وموريشيوس وأستراليا وجورجيا وفرنسا وكندا، بينما حلت روسيا في المرتبة (11).

- وجد التقرير أنه على الرغم من الفجوة الهائلة في الثروة، فإن دول فقيرة مثل ماليزيا وسلطنة عمان كانت أقوى في مجال الأمن السيبراني من بلدان مثل فرنسا وكندا.

- الدول النامية تفتقر إلى خبراء مدربين تدريباً جيداً على الأمن السيبرانى، بالإضافة إلى الإدراك الشامل والتعليم الضروري حول قضايا الأمن السيبرانى لإنفاذ القانون، واستمرار التحديات في الجهازين القضائي والتشريعي.

- دعت الأمم المتحدة إلى وضع استراتيجية الأمن السيبراني كخطوة أولى حاسمة لأي دولة.

- أشار المسح أيضاً إلى أنه لا يوجد معيار عالمي للأمن السيبراني وهو ما يعتبر مشكلة.

وعلى الصعيد العربي يبين الجدول رقم (3) ترتيب الدول العربية للعام 2017م:

الدولة	التقييم
السعودية	(46) عالمياً و (5) عربياً
سلطنة عمان	(4) عالمياً و (1) عربياً
قطر	(25) عالمياً و (3) عربياً
مصر	(14) عالمياً و (2) عربياً
الإمارات	(47) عالمياً و (6) عربياً
الكويت	(138) عالمياً و (17) عربياً
البحرين	(64) عالمياً و (8) عربياً
الأردن	(92) عالمياً و (10) عربياً
تونس	(40) عالمياً و (4) عربياً
المغرب	(49) عالمياً و (7) عربياً
فلسطين	(103) عالمياً و (13) عربياً
السودان	(95) عالمياً و (11) عربياً
العراق	(158) عالمياً و (19) عربياً
الجزائر	(67) عالمياً و (9) عربياً
سوريا	(101) عالمياً و (12) عربياً

الدولة	التقييم
ليبيا	(104) عالميا و (14) عربياً
لبنان	(118) عالمياً و (15) عربياً
موريتانيا	(124) عالمياً و (16) عربياً
الصومال	(161) عالمياً و (21) عربياً
جيبوتي	(139) عالمياً و (18) عربياً
اليمن	(163) عالمياً و (22) عربياً

الجدول رقم (3) المصدر https://www.itu.int/ar/ITU-D/Statisticsh

ثانياً: العام 2018م

وفي النسخة الثالثة الصادرة في العام 2018م اختلفت المؤشرات والأرقام عربياً وعالمياً، وفيما يلي نماذج من الدول العربية التي تغير ترتيبها، بالإضافة إلى ترتيب الدول على المستوى العالمي:

- **المملكة الأردنية الهاشمية:**

تقدم الأردن (18) مرتبة عالمياً، ومرتبتين على المستوى العربي في بيئة الأمن السيبراني، ويتبين أن الأردن تقدم من المرتبة (92) عالمياً إلى المرتبة (74)، ومن المرتبة (10) عربياً إلى المرتبة (8)، حيث شهد الأردن تطوراً ملحوظاً في مجموع درجاته التي بلغت (0.556)، مقارنةً بـ (0.277) في عام 2017م، و (0.206) في عام 2014م.

وصنف التقرير البيئة السيبرانية في الأردن بمرحلة "النضوج"، بعد إصدار الاستراتيجية الوطنية للأمن السيبراني، وإنشاء الفريق الوطني للاستجابة للحوادث السيبرانية (JO-CERT) ، إضافة إلى وجود الشبكة الآمنة للألياف الضوئية.

وأوضح التقرير أن الأردن يعمل على تمكين الإدارة الفاعلة للبيئة الوطنية السيبرانية، فقد ظهر ذلك من خلال إصدار الأردن للاستراتيجية الوطنية للأمن السيبراني، بالإضافة إلى إطلاق مجموعة من السياسات الوطنية للأمن السيبراني التي تعمل على تحسين الإدارة العامة والإدارة الفنية لدى الجهات الحكومية، وإعداد مسوّدة قانون للأمن السيبراني والتي تهدف إلى إنشاء مركز يُعنى بإدارة الأمن السيبراني على المستوى الوطني.

- **المملكة العربية السعودية:**

جاءت المملكة العربية السعودية المركز (13) من بين (175) دولة، وهو يعتبر تقدم إيجابي وإنجاز ملحوظ، حيث تقدمت المملكة العربية السعودية التي حلت الأولى عربياً، (33) مرتبة عن تقييمها في الإصدار السابق للمؤشر العالمي لعام 2017م حيث كان ترتيبها (46) عالمياً.

- **سلطنة عمان:**

حصلت سلطنة عمان على المركز الثاني عربياً. وحازت السلطنة على (0.868) نقطة وجاءت في المركز السادس عشر عالمياً، وقال التقرير أن السلطنة حصلت على درجات عالية الركائز القانونية، وبناء القدرات مشيراً إلى أن السلطنة لديها هيكل تنظيمي قوي، بما في ذلك استراتيجية عالية المستوى للأمن السيبراني وخطة رئيسية وشاملة وخارطة طريق. كما أوضح أن السلطنة أنشأت إطار لعمل الحكومة الإلكترونية، وقال التقرير أن السلطنة أظهرت مقاييس ايجابيه على صحة النظام البيئي والمعروفة باسم (Cyber Green) لقطاعات البنية الأساسية الوطنية للمعلومات، والتي تستهدف تعزيز التواصل والاستجابة للحوادث وقدرات الفرق المشاركة وكذلك ضمان بذل جهد جماعي مستمر للتخفيف من التهديدات السيبرانية بين فرق الاستجابة الوطنية لحوادث الحاسوب (CIRTs) في المنطقة العربية.. وحصلت السلطنة على (0.187) في المعيار القانوني للأمن السيبراني و (0.184) نقطة في المعيار التقني و (0.197) نقطة في المعيار التنظيمي و (0.195) نقطة في مؤشر بناء القدرات و (0.160) في مؤشر التعاون.

- **دولة قطر:**

احتلت المرتبة الثالثة عربياً والسابعة عشر عالمياً وحسب المؤشر الصادر، فقد تقدمت دولة قطر (8) مراكز على مستوى الترتيب العالمي مقارنة بالعام 2017م، بعد أن كانت تحتل المرتبة الخامسة والعشرين عالمياً، وعن استعدادات وتدابير دولة قطر في مجال الأمن السيبراني، أشار التقييم إلى قوة الإطار القانوني والهيكل التنظيمي لدولة قطر ووضع استراتيجية وطنية للأمن السيبراني والتي تركز بشكل رئيسي على تأمين البنية التحتية الحيوية للمعلومات فضلاً عن تأسيس لجنة وطنية للأمن السيبراني تعني بقيادة وتنفيذ الاستراتيجية الوطنية للأمن السيبراني. كما رصد المؤشر أن قانون مكافحة الجرائم الإلكترونية لدولة قطر يتضمن تدابير إجرائية وجنائية معاصرة.

- **دولة الكويت:**

حصلت دولة الكويت على المرتبة (72) للتحقق المركز الخامس خليجياً والسادس عربياً و (67) عالمياً من بين (175) دولة.

الجدول رقم (4) يبين ترتيب الدول العربية للعام 2018م

الدولة	التقييم
السعودية	(13) عالمياً و (1) عربيًا
سلطنة عمان	(16) عالمياً و (2) عربياً
قطر	(17) عالمياً و (3) عربياً
مصر	(23) عالمياً و (4) عربياً
الإمارات	(33) عالمياً و (5) عربياً
الكويت	(67) عالمياً و (6) عربياً
البحرين	(68) عالمياً و (7) عربياً
الأردن	(74) عالمياً و (8) عربياً
تونس	(76) عالمياً و (9) عربياً
المغرب	(93) عالمياً و (10) عربياً
فلسطين	(101) عالمياً و (11) عربياً
السودان	(103) عالمياً و (12) عربياً

الدولة	التقييم
العراق	(107) عالمياً و (13) عربياً
الجزائر	(108) عالمياً و (14) عربياً
سوريا	(114) عالمياً و (15) عربياً
ليبيا	(117) عالمياً و (16) عربياً
لبنان	(124) عالمياً و (17) عربياً
موريتانيا	(145) عالمياً و (18) عربياً
الصومال	(156) عالمياً و (19) عربياً
جيبوتي	(159) عالمياً و (20) عربياً
اليمن	(172) عالمياً و (21) عربياً
جزر القمر	(160) عالمياً و (20) عربياً

الجدول رقم (4) المصدر

https://www.itu.int/ar/ITU-D/Statisticsh

أما على المستوى العالمي فالجدول رقم (5) يبين قائمة بـأعلى (10) دول في العالم في مجال الأمن السيبراني للعام 2018م:

الترتيب	البلد
1	بريطانيا
2	الولايات المتحدة الأميركية
3	فرنسا
4	ليتوانيا
5	استونيا
6	سنغافورة
7	إسبانيا
8	ماليزيا
9	كندا
10	النرويج

الجدول رقم (5) المصدر

https://www.itu.int/ar/ITU-D/Statisticsh

المبحث الثاني

الجهود الدولية والعربية القانونية في تعزيز الأمن السيبراني

أولاً: الجهود التشريعية الدولية لتعزيز الأمن السيبراني

عمل أشخاص المجتمع الدولي على الخروج بعدة قرارات تشريعية لتعزيز الأمن السيبراني وكما يلي:

أ- قرارات الجمعية العامة للأمم المتحدة:

تعمل الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام وتعزيز الأمن السيبراني. وتشارك وكالات الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدد من القضايا، بما في ذلك وضع معايير توفير الحماية لشبكات الانترنت. أما أبرز قرارات الجمعية العامة للأمم المتحدة في هذا المجال فهي:

- القرار 121/45 العام 1990م، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994م.
- القرارات 70/53 في 4 كانون الأول/ ديسمبر 1998م، و49/54 في 1 كانون الأول/ ديسمبر 1999م، 55/ 28 في 20 تشرين الثاني/ نوفمبر 2000م، و 19/56 في 29 تشرين الثاني/ نوفمبر 2001م، و 53/57 في 22 تشرين الثاني/ نوفمبر 2002م، و 32/58 في 18 كانون الأول/ ديسمبر 2003م حول موضوع

"التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي".

- القرارات 63/55 في 4 كانون الأول/ ديسمبر 2000م، و121/56 في 19 كانون الأول/ ديسمبر 2001م، بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات". يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار 239/57 في 20 كانون الأول/ ديسمبر 2002م بشأن "إنشاء ثقافة عالمية للأمن السيبراني".

- قرارات الجمعية العامة 239/57 في 31 كانون الثاني/يناير 2003م و199/58 في 30 كانون الثاني/ يناير 2004م بشأن "إنشاء ثقافة عالمية للأمن السيبراني"، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

- القرار CCPCJ 16/2/2007 من نيسان/ أبريل 2007م "المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال" (الفقرات 7، 16).

- قرار المجلس الاقتصادي والاجتماعي E/ 2007/20 بتاريخ 26 تموز/ يوليو 2007م بعنوان "التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية" (E/2007/30 وE/2007/SR.45).

- قرار المجلس الاقتصادي والاجتماعي 26/2004 بتاريخ 21 تموز/ يوليو 2004 بعنوان «التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة».

- الفقرة (18) من "إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين"، التي أقرتها الجمعية العامة في القرار 59/55 المؤرخ 4 كانون الأول/ ديسمبر 2000م، والفقرة 36 المرفقة بقرار الجمعية العامة 261/56 المؤرخ 31 كانون الثاني/ يناير 2002م حول: "خطط العمل لتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين".

- الفقرتان (15 و 16) من إعلان بانكوك بشأن "أوجه التآزر والتعاون: التحالفات الاستراتيجية في مجال منع الجريمة وتحقيق العدالة الجنائية"، الذي أقرّه قرار الجمعية العامة 177/60 بتاريخ 16 كانون الأول/ ديسمبر2005م.

- توصيات مؤتمر ورشة العمل على "التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر"، الذي عقد في بانكوك في 22 نيسان/ أبريل 2005م كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية. الفقرة (2) من قرار الجمعية العامة 177/60 التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

- قرار لجنة مكافحة المخدرات 5/48 حول "تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات".

- الفقرة (17) من قرار الجمعية العامة 178/60 المؤرخ 16 كانون الأول/ ديسمبر 2005م، بخصوص "التعاون الدولي لمكافحة مشكلة المخدرات العالمية".

- قرار لجنة مكافحة المخدرات 8/43 في 15 آذار/ مارس 2000م عبر الإنترنت.

- قرار المجلس الاقتصادي والاجتماعي 42/2004 بشأن "بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت".

- في 2004م تم إنشاء مجموعة الخبراء الحكومية (GCE)، بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية، التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية، كما شكل الأمين العام للأمم المتحدة كوفي عنان في 2004م فريقاً دولياً لدراسة قضية إدارة الانترنت. (العدوان، رائد، "المعالجة الدولية لقضايا الإرهاب الإلكتروني "، 2016م، ص 9-10)

- مختلف توصيات الهيئات الفرعية التابعة للجنة مكافحة المخدرات واللجنة الفرعية المعنية بالاتجار غير المشروع بالمخدرات والمسائل المتعلقة بالشرقين الأدنى والأوسط.

- التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت العام 2005م، وتوصيات للحد من انتشار المبيعات غير المشروعة من المواد الخاضعة للرقابة ولا سيما المستحضرات الصيدلانية، عبر الإنترنت.
- هنالك تعاون بين المكتب المعني بالمخدرات والجريمة (UNODC) في الأمم المتحدة، والاتحاد الدولي للاتصالات، لمساعدة الدول الأعضاء في الاتحاد، للحد من المخاطر التي تشكلها الجريمة السيبرانية، وذلك بموجب مذكرة تفاهم موقعة بين المنظمتين، في منتدى القمة العالمية لمجتمع المعلومات. (**UN and ITU team up to fight Cybercrime** By Messaging News staff)

ب- اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976م. وفي العام 1996م، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية. عملت اللجنة بين العامين 1997م و 2000م على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان/ أبريل 2001م. وتم التصديق على الاتفاقية من قبل (30) دولة بحلول العام 2010م، إن اتفاقية جرائم اللإنترنت هي المعاهدة الدولية الأولى التي

تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى.

وتهدف الاتفاقية إلى:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي.
- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.
- تتضمن أيضاً الاتفاقية المبادئ العامة المتعلّقة بالتعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.
- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.
- الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

وكان المجلس الأوروبي، قد أقر معاهدة مكافحة الجريمة السيبيرية، التي دخلت حيز التنفيذ، سنة 2004م، (انظر: الموقع الإلكتروني) داعياً جميع الدول إلى التوقيع عليها، منذ تاريخ إقرارها في العام 2001م. وتعتبر أحكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة السيبرانية، لاسيما وأنها تطلب من الدول الأعضاء، إنشاء مراكز اتصال، تعمل بحسب مبدأ استمرارية الخدمة، أي تأمين متابعة على امتداد ساعات اليوم، بحيث تكون دائمة الاستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية.

ت- مجموعة الدول الثماني: (8G)

اعتمد وزراء العدل والداخلية التابعين لبلدان الـ (8G) في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية: عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، تدريب الموظّفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

بالإضافة إلى ذلك، دعت دول الـ (8G) إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة، ومن تثمير الدراسات العديدة التي وضعتها دول الـ (8G) ومن بينها:

مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (1997م)، ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (1999م)، وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (2002م)، ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (2002م)، وإعلان بيان دول (**8G**) على نظم حماية المعلومات (2002م).

وترى دول الـ (**8G**) أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلّب الاتصال والتنسيق والتعاون داخليًا ودوليًا بين جميع أصحاب المصلحة في القطاع الخاص والأوساط الأكاديمية، والمؤسسات الحكومية. بناءً على ذلك، فإن دول الـ (**8G**) التزمت تدريب جميع العاملين في مجال تطبيق القانون وتجهيزهم بالمعدات الضرورية لمكافحة جرائم الإنترنت. كما تعهّدت بمساعدة جميع البلدان الأعضاء على إقامة مراكز اتصال تعمل على مدار (24) ساعة سبعة أيام في الأسبوع. إن وجود جرائم تعتمد التكنولوجيا المتقدّمة تطرح تحديات كبيرة على الأجهزة القضائية. فغالبًا ما يكون من الصعب على المحققين ذات المهارة العالية العمل بسرعة فائقة لحماية البيانات الالكترونية وتحديد المتهمين بخرق القانون. من هنا أهمية الشبكة التي طرحت دول الـ (**8G**) إنشاءها، لأنها ستمكّن من الاستجابة بسرعة كبيرة لطلبات السلطات الرسمية أو مستخدمي شبكات الانترنت.

إن توصيات الـ (8G) بالنسبة لجرائم التكنولوجيا المتقدمة والجرائم ذات الصلة بالكمبيوتر موجودة في إطار الباب (D) من المعاهدة وتتلخص بما يلي:

- يتعيّن على الدول أن تُجرِّم الانتهاكات على حقوق الغير الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي في ما يتعلّق بمكافحة هذه الانتهاكات.
- ينبغي للدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:
- التعاون مع القطاع الصناعي لضمان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الالكترونية للهجمات.
- سن قوانين وتدابير أخرى وتنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير والقرصنة.
- تحديد المشاكل المحتملة ومعالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.
- نشر الوعي العام في ما يتعلق بموضوع الجريمة ذات التقنية العالية.
- يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق

والادعاء العام، من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيا الكمبيوتر لارتكاب جرائمهم. ويتوجّب على الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.

- ينبغي تحسين التواصل بين الموظفين المكلّفين تطبيق القوانين في مختلف الدول، بما في ذلك تبادل الخبرات في معالجة هذه المشاكل.
- يتوجب على الدول الحفاظ على التوازن المناسب بين حماية الحق في الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.
- على الدول تشجيع وضع القوانين وتنفيذ تدابير لتوفير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسي على الإنترنت.

ثانياً : التعاون العربي في المجال القضائي

- ✓ اتفاقية الرياض للتعاون القضائي العربي لسنة 1984م.
- ✓ اتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الجرائم الإلكترونية.
- ✓ الاتفاقيات الثنائية لتسليم المجرمين.
- ✓ الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات 2010م، تم توقيعها من قبل وزراء الداخلية والعدل العرب في مصر.

ثالثاً : الجهود التشريعية العربية لتعزيز الأمن السيبراني

لم تتوانى الدول العربية في مواكبة متطلبات الأمن السيبراني حيث سارعت الدول إلى سن القوانين والتشريعات التي تسعى لتعزيز الأمن السيبراني ومواجهة الجريمة السيبرانية بكافة أشكالها والتي اندرجت بمسميات مختلفة وفيما يلي عرض لنماذج من الجهود العربية في هذا الاتجاه :

- **المملكة الأردنية الهاشمية:** قانون الجرائم الإلكترونية رقم 27 لسنة 2015م، وفي شهر 7 من العام 2019م أقر مجلس النواب الأردني بأغلبيته، قانون الأمن السيبراني "مكافحة الهجمات الالكترونية"، ووافق المجلس في هذا القانون الجديد على تأسيس جسمين جديدين في هيكل الحكومة وهما: المجلس الوطني للأمن السيبراني، والمركز الوطني للأمن

السيبراني، ويتيح هذا القانون تأسيس شركات أو مؤسسات خاصة تقدم الأنشطة الفنية والإدارية والاستشارية في مجال الأمن السيبراني بما فيها خدمات التقييم الأمني والمراقبة والتدقيق والخدمات الاستشارية.

- **الإمارات العربية المتحدة:** يعد القانون الاتحادي رقم 2 لسنة 2006م من القوانين النموذجية التي تطرقت إلى أغلب الجرائم المعلوماتية. وهو أول قانون في الدول العربية يصدر بشكل مستقل لمواجهة الجرائم المعلوماتية. وبتاريخ 13 أغسطس 2012م صدر القانون الإماراتي الاتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات، وبموجب المادة (50) منه ألغي القانون الاتحادي رقم 2 لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات القانون الاتحادي رقم 5 لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات.

- **المملكة العربية السعودية:** نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 1428/3/8هـ

- **سلطنة عُمان:** يجرِّم قانون مكافحة جرائم تقنية المعلومات رقم 12 لسنة 2011م، التعدي على سلامة وسرية بيانات أو معلومات إلكترونية حكومية سرية، أو البيانات والمعلومات الإلكترونية السرّية الخاصة بالمصارف والمؤسسات المالية، وتداول المواد الإباحية وتحريض أو إغواء ذكر أو أنثى لارتكاب الفجور أو الدعارة،

التهديد أو الابتزاز، نشر أفكار ومبادئ تنظيم إرهابي، ونشر طرق صناعة المتفجرات والأسلحة، وغسل الأموال، الاتجار غير المشروع بالآثار، والتعدّي على حق المؤلف. كما يعاقب على الاعتداء على حرمة المشروع بالآثار، والتعدّي على حق المؤلف. كما يعاقب على الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، أو الإخلال بالآداب العامة، أو في الترويج لبرامج أو أفكار أو أنشطة من شأنها ذلك. أما بالاتجار بالمخدرات وحسب نص المادة (25) فيعاقب بالإعدام أو بالسجن المطلق وغرامة لا تقل عن (25) ألف ريال عُماني ولا تزيد عن (100) ألف ريال كل من انشأ موقعاً إلكترونياً، أو نشر معلومات على الشبكة المعلوماتية أو وسائل تقنية المعلومات بقصد الاتجار أو الترويج للمخدرات.

- **دولة الكويت:** توجد في الكويت ثلاثة قوانين رئيسة حول الجرائم المرتكبة بوسائل تقنية المعلومات وهي: قانون رقم (8) لسنة 2016م بشأن تنظيم الإعلام الالكتروني، وقانون جرائم تقنية المعلومات وقانون الاتصالات.

- **دولة قطر:** يعاقب قانون مكافحة الجرائم الالكترونية رقم (14) لسنة 2014م، كل من أنشأ أو أدار موقعاً لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو الترويج لأفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية. كما يحظر نشر أخبار غير صحيحة، بقصد تعريض سلامة الدولة أو نظامها العام

أو أمنها الداخلي أو الخارجي للخطر. ويحظر بث أو حيازة مادة إباحية عن طفل بواسطة وسائل تقنية المعلومات، والاعتداء على حرمة الحياة الخاصة أو العائلية للأشخاص؛ولو كانت صحيحة، أو تعدّى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، أو تهديد أو ابتزاز شخص، لحمله على القيام بعمل أو الامتناع عنه.

- **مملكة البحرين:** يجرِّم قانون رقم (60) لسنة 2014م بشأن جرائم تقنية المعلومات وتعديلاته استخدام الانترنت لنشر أي مضمون إباحي. وتشدّد العقوبة إذا كانت المادة الإباحية موجهة إلى الأطفال. وتنص المادة: فيما عدا ما ورد بشأنه نص خاص في هذا القانون، من قام بارتكاب جريمة منصوص عليها في أي قانون آخر بواسطة نظام أو أي وسيلة تقنية معلومات، يعاقب بالعقوبة المقررة لتلك الجريمة. ويعاقب قانون العقوبات البحريني الصادر بالمرسوم بقانون رقم (15) لسنة 1976م كل مواطن أذاع عمداً في الخارج أخباراً أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للدولة، وكان من شأن ذلك إضعاف الثقة المالية بالدولة، أو النيل من هيبتها أو اعتبارها، أو باشر بأي طريقة كانت نشاطاً من شأنه الإضرار بالمصالح القومية.

- **الجمهورية العربية السورية:** قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم (17) لسنة (2012 م).

- **السودان:** قانون جرائم المعلوماتية الصادر عام 2007م، ويشترك تقريباً مع أغلب ما جاء في قوانين الدول العربية.

- **الجزائر:** القانون رقم (04 – 09) المتضمن قواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- **موريتانيا:** يتوافق القانون رقم (007 – 2016) المتعلق بالجريمة السيبرانية مع معظم القوانين العربية في تجريم الإباحية، بخاصة إذا كانت موجهة للأطفال، والتعدي على الخصوصية ونشر الأسرار ذات الصلة بالدفاع والأمن الوطني. وعن قضايا العرق والتمييز تنص (المادة 1 فقرة 3) من الدستور: " يعاقب القانون كل دعاية إقليمية ذات طابع عنصري أو عرقي".

ومن نافلة القول أن هنالك قوانين خاصة صدرت في الدول العربية تعنى بمكافحة غسيل الأموال وبعض الجرائم المالية الأخرى، الخاصة بالتحويلات المالية والمصرفية، مثل قانون رقم (46) لعام 2007م الصادر في الأردن، وقانون 2004م في عمان، ونظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال في لبنان، وقانون عام 2003م الصادر في اليمن، إضافة إلى تفرد دبي بقانون 2004م الخاص بمكافحة الجرائم الإرهابية، وتونس بالقانون رقم (75) الخاص بدعم الجهود الدولية في مكافحة الإرهاب وتبييض الأموال، الصادر عام 2003م والمعدل في العام 2009م.

وفي مقارنة بين قوانين الجرائم الإلكترونية في الدول العربية، نجد أنها أولاً تتفق مع بعضها البعض وثانياً مع عدد من الدول الأجنبية في تجريم الأفعال التالية:

(الدخول غير المشروع إلى أي نظام أو شبكة معلوماتية بهدف تغيير البيانات أو المعلومات، تعطيل أي موقع أو خدمة إلكترونية، حماية المراسلات والاتصالات للأفراد، نشر مواد إباحية حول الأطفال، تزوير توقيع إلكتروني، الاستيلاء على ما أو بيانات بطاقة ائتمانية باستعمال طرق احتيالية، الاتجار بالبشر، ترويج المخدرات، غسيل الأموال، القمار، الإرهاب وترويج أفكار منظمة إرهابية أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، الحصول على معلومات حكومية سرية).

المبحث الثالث

المؤتمرات الدولية لتعزيز الأمن السيبراني

كما ذكرنا سابقاً إن الدول لم تدخر جهداً في بذلها لغايات تعزيز الأمن السيبراني لبلدانها والمجتمع الدولي، وتهدف هذه الجهود إلى مكافحة أخطار الفضاء السيبراني، وتتعدد أنواع هذه الجهود، حيث لا تقتصر على سن وتشريع القوانين، بل تتعداها إلى عقد اللقاءات والاجتماعات التشاورية والتي من خلالها يتم تبادل والاستماع إلى وجهات النظر المختلفة، وفي هذا المبحث سيتم التعرف على أبرز المؤتمرات واللقاءات بين الدول التي تعنى بالأمن السيبراني وأمن تكنولوجيا المعلومات حيث سيتم تقسيمها إلى مؤتمرات الأمم المتحدة ولقاءات دولية وأوروبية أخرى ومؤتمرات ولقاءات عربية وكما يلي:

أولاً: مؤتمرات الأمم المتحدة

1- مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام 1990م.

2- مؤتمر الأمم المتحدة العاشر الذي صدر في فيينا عام 2000م .

3- توصيات مؤتمر ورشة العمل على " التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر "، الذي عقد في بانكوك في 22 نيسان/ إبريل 2005م كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية.

4- ورشتي عمل حول مكافحة استخدام الإرهابيين للإنترنت (18-2009/10/19م) ومنع الإرهابيين من حيازة واستخدام أسلحة الدمار الشامل أو مكوناتها (20-2009/10/21م)، وقد عقدتا بمشاركة الأمانة العامة لمجلس وزراء الداخلية العرب وخبراء من الدول العربية والأمم المتحدة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والمنظمات الإقليمية والدولية المعنية وصدر عن كل منهما مجموعة من التوصيات.

5- مؤتمر الأمم المتحدة الثاني عشر- البرازيل - سلفادور عقد عام 2010م، غطى ثمان مسائل منها مشاكل جرائم الإنترنت أو الشبكة العنكبوتية.

6- مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية (2-12) نيسان/ ابريل لسنة 2015م المنعقد في الدوحة.

ثانياً : مؤتمرات ولقاءات دولية وأوروبية أخرى

1- خطة عمل لندن: استضافت لجنة التجارة الاتحادية ومكتب التجارة النزيهة في المملكة المتحدة مؤتمراً دولياً بشأن الإنفاذ فيما يتعلق بالرسائل الاقتحامية في لندن عام 2004م. وقد أدى هذا المؤتمر إلى وضع خطة عمل لندن بشأن التعاون الدولي في الإنفاذ ذي الصلة بالرسائل الاقتحامية، والغرض من خطة عمل لندن هو تعزيز التعاون الدولي في مجال الإنفاذ بشأن الرسائل الاقتحامية

ومعالجة المشاكل ذات الصلة بهذه الرسائل مثل الاحتيال والخداع على الخط مباشرة وعمليات الاحتيال ونشر الفيروسات.

2- (Annual Computer Security Application Conference ((ACSAC)): هو المؤتمر السنوي لتطبيقات أمان الكمبيوتر - ويعد أقدم مؤتمر لأمن المعلومات يعقد سنوياً.

3- مبادرة عمل وارسو: عقد ممثلو أكثر من (40) دولة مجموعة عمل معنيّة بأمن الفضاء السيبراني في الفترة من 7 إلى 8 تشرين الأول من العام 2019م في سول، كوريا الجنوبية، لمناقشة استراتيجيات الردع والهجمات الإلكترونية بشكل أفضل.

4- المؤتمر العالمي لتنمية الاتصالات في حيدر آباد، الهند، (WTDC-10)، في يونيو 2010م. و كان من بين المقررات أن الاتحاد ينبغي أن يساعد الدول الأعضاء، وخصوصاً البلدان النامية، في وضع التدابير القانونية المناسبة والعملية المتصلة بالحماية من التهديدات السيبرانية.

5- القمة العالمية لمجتمع المعلومات التي عقدت في جنيف، 10-12 ديسمبر 2003م.

6- مؤتمر قمة الأمن السيبراني مينابولس، مينيسوتا، الولايات المتحدة الأمريكية 22-21 أكتوبر 2014م. شارك فيه ممثلي من القطاعين العام والخاص لمناقشة التدابير المضادة للتهديدات الإلكترونية، وتعزيز أمن القطاع العام والخاص في مواجهة الجريمة الإلكترونية وقياس مدى تأمين برامج الحاسب الآلي ضد الهجمات

وتطوير تحقيقات الشرطة ومهارات التحقيق التقنية والأدلة العلمية والاستراتيجيات الشاملة لمواجهة الجريمة الإلكترونية.

7- مؤتمر الإنتربول واليورو بول الثاني للجريمة الإلكترونية سنغافورة 3-1 أكتوبر 2014م (INTERPOL/EUROPOL Cybercrime Conference، دعمت عقد هذا المؤتمر أحد الجهات الاعتبارية الدولية الفاعلة في مكافحة الجريمة الإلكترونية وتعرف بـ "الجهود الدولية في الجريمة الإلكترونية"، وتسمى اختصاراً (GLACy)(120) ، وقد أسهمت بدعمها بتمكين خبراء في الجريمة الإلكترونية من أكثر عشرين دولة من المشاركة في المؤتمر الذي يهدف إلى تسهيل مهمة الوحدات المتخصصة في مكافحة الجريمة الإلكترونية في الاتصال بين بعضها البعض من خلال الشبكة الدولية (International Networking)

8- مؤتمر الأمن السيبراني/ جامعة نيويورك للتكنولوجيا 18 سبتمبر 2014م: شارك في هذا المؤتمر خبراء الإنترنيت والشركات والحكومات وناقش المؤتمر الموضوعات التالية: الخصوصية - الابتكارات في المؤسسة الأجنبية - أنظمة الأمن والإنترنت حماية البنية التحتية الحساسة والمنظمات والأفراد من الهجمات الإلكترونية .

9- مؤتمر (GLACY) لبناء القدرات في بور لويس عاصمة جزر موريشيوس 14-11 أغسطس 2014م:(GLACY :Capacity Building in Mauritius – Conference and

workshops) عقد هذا المؤتمر تحت رعاية (الجهود الدولية في الجريمة الإلكترونية)GLACY ، وقام مجلس أوروبا للجريمة الإلكترونية بدعم سلسله من نشاطات بناء القدرات في الفترة من 14-11 أغسطس 2014م، وناقشت ورش العمل والمؤتمر الموضوعات التالية: اتفاقية مجلس أوروبا للجريمة الإلكترونية. ومدى إمكانية حصول سلطات إنفاذ القانون على المعلومات، (Law enforcement access to data)، واستراتيجيات تدريب منتسبي سلطات إنفاذ القانون ومنتسبي السلطات القضائية. وحماية الطفل. وإعادة النظر في القانون الجنائي لمواكبة مقتضيات مكافحة الجريمة الإلكترونية، والتعاون الدولي. (الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، ص71-72، مصدر سابق.)

-10 المؤتمر العالمي الرابع " للفضاء الإلكتروني" الذي انعقد في مدينة لاهاي بهولندا خلال الفترة 16-17 أبريل لعام 2015م.

-11 (Con An Infosec) : هو المؤتمر التدريبي الذي يحدث سنوياً في لندن، المملكة المتحدة.

-12 (ACM-CCS): هو مؤتمر الأمن الذي عقد منذ عام 1993م حول أمن الكمبيوتر والاتصالات.

-13 :(ASIA)هي الندوة السنوية حول ضمان المعلومات التي تعد بمثابة المسار الأكاديمي لمؤتمر الأمن السيبراني لولاية نيويورك، وهو مؤتمر سنوي لأمن المعلومات يعقد في نيويورك عادة لمدة

يومين خلال شهر يونيو، يستهدف المشاركين الأكاديميين والحكوميين والصناعيين

14- (Black Hat) : هي سلسلة من المؤتمرات التي تعقد سنويا في مدن مختلفة في جميع أنحاء العالم وتعد (Black Hat USA) ، التي عقدت في لاس فيجاس من قبل (DEF CON) ، واحدة من أكبر أحداث أمان الكمبيوتر في العالم.

15- (BlueHat) : وهو مؤتمر أمان (Microsoft) يتم الدعوة إليه مرتين فقط في العام، يهدف إلى الجمع بين محترفي الأمن في (Microsoft) والباحثين في مجال الأمن الخارجي.

16- (Brucon) : هو مؤتمر سنوي، يعقد في مدينة غنت البلجيكية، منذ عام 2012م، يستمر هذا المؤتمر لمدة يومين، ويسبقه فترة تدريب أيضاً.

17- (CanSecWest): يقام هذا المؤتمر في مدينة فانكوفر الكندية في نهاية شهر آذار ويستضيف مسابقة القرصنة.

18- (CSS): هو المؤتمر الدولي لنظام التشفير والأمن والمنعقد سنوياً في بولندا.

19- (DeepSec): هذا المؤتمر يُعقد في العاصمة النمساوية فيينا، ويغطي العديد من الجوانب الأمنية للحوسبة والاتصالات الإلكترونية، وكذلك إدارة الأمن والجوانب الاجتماعية. ويشارك فيه جمهور دولي واسع، على سبيل المثال: أكاديميين، باحثين،

بائعين، ومُمولين، إدارة عامة وما إلى ذلك (يخضع لتدريب لمدة يـومين، ومؤتمر لمدة يومين).

20- (Department of Defence Cyber Crime Conferenc): هـو مؤتمر سنوي يركز على احتياجات أمن الكمبيـوتر للحكومـة الفيدراليـة والجيش والدفاع في الولايات المتحدة.

21- (FSec): هو مؤتمر الأمن السنوي الكرواتي الذي يُعقد في كلية التنظيـم والمعلوماتية في مدينة فارازدين الكرواتية.

22- (GreHack.fr): هو مؤتمر سنوي يعقد في مدينة غرينوبـل الفرنسـية، المشاركين هم من فئـات الأوسـاط الأكاديميـة والصـناعية. أيضـاً هنـاك مشاركين في كل من مختصين الأمن الهجومي والدفاعي لأمان الحاسب.

23- (Hacker Halted): هـو مـؤتمر مُقـدم مـن المجلـس الأوروبي (EC-Council) ويتضمن السلسلة العالمية لمؤتمرات هاكر هالـدت وهـدفها هو زيادة الوعي الدولي بزيادة التعليم والأخلاقيات في أمن تكنولوجيـا المعلومات

24- (HackinParis): هـــو حـــدث ومـــؤتمر ســنوي تنظمـــه شركـــة (SYSDREAM) في العاصمة الفرنسية باريس وتشتمل أعمال المـؤتمر على أمن تكنولوجيا المعلومات، والتجسس الصناعي، واختبار الاخـتراق، والأمـن المـادي، والهندسـة الاجتماعيـة، والتحليـل والأدلـة الجنائيـة، وتقنيات تحليل البرامج الضارة والتدابير المضادة.

25- (Hackito Ergo Sum): هذا المؤتمر يُعقد في باريس في أبريل من كل عام ويُناقش فيه قضايا مهمة وجوانب عدة مثل الجانب الهجومي والدوائر الأكاديمية المتعلقة في أمان الحاسب.

26- (HITBSecConf / Hack In The Box) : وهو مؤتمر أمن المعرفة العميقة الذي يُعقد في ماليزيا وهولندا.

27- (ICISSP): هو المؤتمر الدولي الذي يهتم حول أمن وخصوصية نظم المعلومات ويعقد بشكل سنوي لمدة يومين منذ العام 2015م في البرتغال.

28- (INFWARCON): هو مؤتمر يدور ويغطي حقائق خلف حرب المعلومات، وهو أيضاً مؤتمر التدريب على الأسلحة والتكنولوجيا السيبرانية.

29- (IP EXPO Europe): هو مؤتمر يُعقد سنويًا في مركز (ExCeL) في لندن.

30- (IP EXPO Nordic): هو مؤتمر يُعقد سنويًا في مركز (Waterfront) للمؤتمرات في ستوكهولم.

31- (RSA Security Conference): وهو مؤتمر التشفير وأمن المعلومات المتعلق بأمن البيانات، والذي يُعقد سنويًا في منطقة خليج سان فرانسيسكو.

32- (SecureWorld Expo): وهو عبارة عن سلسلة من مؤتمرات أمن تكنولوجيا المعلومات التي توفر التعليم وفرص التدريب

على CPE والتواصل بين قادة الأمن والخبراء وكبار المسؤولين التنفيذيين وصناع السياسة الذين يشكلون وجه الأمن.

33- (SOURCE Conference): هو مؤتمر أمان الكمبيوتر في بوسطن ودبلن وسياتل، وهو يقدم التعليم في كل من الجوانب التجارية والفنية لصناعة الأمن.

34- (Positive Hack Days): هو الحدث الدولي السنوي لأمن تكنولوجيا المعلومات ويُعقد مع ورش العمل التي عقدت في موسكو، روسيا.

ثالثاً: مؤتمرات ولقاءات عربية

1- مؤتمر قمة الأمن السيبراني - مملكة البحرين 22- 20 أكتوبر 2014م. ناقشت هذه القمة الموضوعات التالية: بحث سبل إعادة الأمن واستراتيجيات تكنولوجيا المعلومات. وإعادة تعريف المخاطر. وتنفيذ أفضل الممارسات لتحقيق مدونه التهديدات. وتخفيف مخاطر أدوات التواصل الاجتماعي الجديدة. وإستراتيجية مواجهة التهديدات المتنقلة. والاستغلال الجنسي للأطفال.

2- المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية الذي نظمته جامعة الأمام محمد بن سعود الإسلامية ممثلة في كلية علوم الحاسب والمعلومات وذلك في الفترة من 10 إلى 12 نوفمبر 2015م.

3- مؤتمر الأمن السيبراني الخليجي الثاني والذي انعقد في دولة الكويت 2019م، حيث دعا خبراء في أمن المعلومات إلى ضرورة توحيد

الجهود الخليجية لمواجهة تحديات الأمن السيبراني، وتوفير الحماية اللازمة للبيانات والمعلومات الحساسة الخاصة بدول مجلس التعاون الخليجي عبر وضع إستراتيجيات وطنية لمواجهة تلك التحديات.

4- "المؤتمر الدولي حول **الأمن السيبراني**" والمنعقد في العاصمة الأردنية عمان خلال الفترة 21-20 مارس 2019م، حيث عقد هذا المؤتمر بتنظيم من هيئة تنظيم قطاع الاتصالات الأردنية بالتعاون مع مجموعة عرب للقانون ومركز الشرق الأوسط للاستشارات والدراسات.

5- مؤتمر الأمن السيبراتي (CYBPOS Amman 2019)، والمنعقد في العاصمة الأردنية عمان، برعاية سمو الأميرة سمية بنت الحسن، بهدف نشر الوعي بالمفاهيم الخاصة به على مستوى الأفراد والمؤسسات، وتم خلال المؤتمر عرض قانوني الأمن السيبراني والجرائم الإلكترونية، والمفاهيم والمشاكل والتحديات والحلول الخاصة بالأمن السيبراني، وتكنولوجيا بلوكتشين (BlockChain) من وجهة نظر الأمن السيبراني، إلى جانب الحديث عن الجرائم الإلكترونية والأدلة الجنائية الرقمية، والاختراق الأخلاقي، والثغرات ونقاط الضعف في الشبكات والتطبيقات والبرمجيات، والبرامج الخبيثة والاختراق والمخاطر.

6- "قمة الأمن السيبراني" في الدوحة بالشراكة بين مؤتمر ميونخ للأمن واللجنة الوطنية القطرية للأمن السيبراني 2020م، بمشاركة ممثلين رفيعي المستوى عن حكومات ومؤسسات دولية وأعمال تجارية

وأوساط أكاديمية وعسكرية، لمناقشة قضايا الأمن الإقليمي والعالمي، وزيادة الوعي بقضايا الأمن السيبراني وتداعياتها وتأثيراتها بنموذج الحكم الدولي.

7- "أعمال المؤتمر الدولي للأمن السيبراني وحماية المؤسسات العربية من الاختراقات"، ويعقد المؤتمر مشاركة دول عربية بالتعاون مع منظمة الايسيسكو ويمثل هذه الدول خبراء ومختصين في مجال الأمن السيبراني.

8- " الأسبوع الإقليمي للأمن السيبراني في المنطقة العربية " والمنعقد في العاصمة العمانية مسقط في الفترة من 27 إلى 31 أكتوبر 2019م ويأتي تنظيم هذا الأسبوع بهدف تبادل الخبرات وتوطيد وتعزيز التعاون بين الدول العربية في مجال السلامة المعلوماتية عموماً وتحديد آليات واضحة للتعامل مع الهجمات والتهديدات في الفضاء السيبراني العربي والدولي.

9- "المؤتمر الأول للأمن السيبراني" المنعقد في المملكة الأردنية الهاشمية بشهر 8 من العام 2019م، والذي يتضمن أحدث أنواع التكنولوجيا في مجال الأمن والجرائم الإلكترونية والأدلة الجنائية الرقمية، وذلك بمشاركة نخبة من العلماء والخبراء على المستوى الدولي وكبرى الشركات العالمية المتخصصة. ويسعى المؤتمر إلى تحقيق جملة من الأهداف، أبرزها التعريف بقانون الأمن السيبراني الأردني 2019م، وقانون الجرائم الإلكترونية، وتعزيز الأمن

السيبراني، ونشر الوعي بالمفاهيم الخاصة بالأمن السيبراني على مستوى الأفراد والمؤسسات.

10- " مؤتمر الأمن السيبراني" (CDS) : والذي عقد في الرياض عاصمة المملكة العربية السعودية الرياض بين 13 و14 فبراير 2019م، ويهدف إلى مناقشة سبل المعالجة الاستباقية لتحديات الأمن السيبراني وكيفية حماية البيانات والمعلومات الحساسة للمملكة العربية السعودية , ويجمع أكثر من (600) من صناع القرار والمسؤولين وكبار المدراء في المجال السيبراني (كبار مسؤولي المعلومات، وكبار مسؤولي أمن المعلومات، مدراء تقنية المعلومات، مدراء الخصوصية)، بالإضافة إلى أكثر من (50) متحدثًا وأكثر من (30) مزوّد حلول، وتشمل القطاعات الرئيسية المعنية القطاع الحكومي والدفاع والقوات شبه العسكرية، البنوك والخدمات المالية والتأمين، الطاقة والمرافق، التصنيع، تجارة التجزئة وسلسلة التوريد، المستشفيات، الجامعات، التكتلات المتنوعة، وقطاع العقار والتشييد. من ناحية أخرى، تغطي الحلول المهمة: الحماية من البرامج الضارة، أمن السحابة الإلكترونية، أمن أنظمة المراقبة الصناعية، أمن المدفوعات، الحماية ضد هجمات حجب الخدمة، أمن إنترنت الأشياء، الخدمات الأمنية المدارة، الحماية ضد فقدان البيانات (DLP)، إدارة الوصول الخاص وأمن الطرفيات.

11- " مؤتمر الدفاع السيبراني 2019م (فاير آي) بدبي ": بمشاركة واسعة ناقش المؤتمر أهم الممارسات الكفيلة باكتشاف الهجمات

السيبرانية والتصدي لها، ويهدف المؤتمر إلى تعريف المشاركين بأحدث التهديدات السيبرانية، وكيفية حماية المؤسسات من الاختراقات السيبرانية المحتملة، كما يشكل المؤتمر فرصة للقاء الاختصاصيين والقادة في مجال الأمن السيبراني، وخلق جو ملائم للتعاون بين المنظمات والمؤسسات فيما يخص مجال الأمن السيبراني.

المبحث الرابع

المؤسسات والمراكز المعنية بالأمن السيبراني

سعت الدول كل حسب إمكانياتها إلى افتتاح المؤسسات والمعاهد والمراكز التي تعنى بالأمن السيبراني حيث تقوم هذه المؤسسات والمعاهد على العمل على تأهيل جيل جديد قادر علمياً وتطبيقياً على التعامل مع تهديدات الفضاء السيبراني بأشكالها المختلفة، بالإضافة إلى مواكبة التطورات والمخاطر ومواجهتها في مجال الأمن السيبراني وخصوصاً في حالات الطوارئ، وفي هذا المبحث تسليط الضوء على ما أمكن من مؤسسات ومعاهد تعنى بالأمن السيبراني مع الأخذ بعين الاعتبار أن الدول الكبرى تضم مراكز عديدة حيث سنأخذ أبرز المراكز أو الوكالات في هذه الدول وكما يلي:

أولاً: المراكز الدولية و الأجنبية

1- **منظمة:(CCD COE)** تتبع لحلف الناتو ويقع مقرها بمدينة تالين باستونيا وتأسست في العام 2008م، وهي منظمة عسكرية دولية مستقلة عمليًا، وتم تمويلها من قبل الدول المشاركة لتركز على البحث والتطوير والتدريب والتعليم في كل من الجوانب التقنية وغير التقنية للدفاع السيبراني.

2- **الولايات المتحدة الأمريكية:** تجدر الإشارة أن الولايات المتحدة الأمريكية كانت من أوائل الدول التي بدأت في التعامل مع الأمن

السيبراني كمهمة استراتيجية، حيث تبنت وزارة الدفاع الأمريكية في العام 1967م برنامجاً يطلق عليه أربانت، كان الراعي المباشر له هو "وكالة مشروعات البحوث المتقدمة" الجهة المسؤولة عن تطوير واستحداث أسلحة مستقبلية لجيش الولايات المتحدة. وكان الهدف من "أربانت" هو إتاحة وسيلة للمتعاقدين مع الوكالة (العلماء في المختبرات والجامعات في جميع أنحاء البلاد) لتشارك البيانات والأوراق البحثية والاكتشافات على شبكة حاسوبية واحدة، ونظراً للعدد الكبير من المراكز الأمريكية البحثية والتدريبية في مجال الأمن السيبراني. نشير هنا إلى وكالة الأمن السيبراني وأمن البنية التحتية (Cybersecurity and Infrastructure Security Agency) :(CISA) أنشأت بتاريخ 16 نوفمبر 2018م عندما وقع الرئيس الأمريكي دونالد ترامب على قانون وكالة الأمن السيبراني وأمن البنية التحتية لعام 2018م ليصبح قانونًا، وهي وكالة فدرالية مستقلة في الولايات المتحدة تحت إشراف وزارة الأمن الداخلي وتعتبر أنشطتها استمرار للمديرية الوطنية للحماية والبرامج (NPPD)، وهو برنامج أنشئ في عام 2007م داخل وزارة الأمن الوطني. تشرف وكالة الأمن السيبراني وأمن البنية التحتية على: (قسم الأمن السيبراني، قسم اتصالات الطوارئ، خدمة الحماية الفيدرالية، ((FPSقسم البنية التحتية، المركز الوطني لإدارة المخاطر)، بلغت ميزانية المركز (1.5) مليار دولار للإعداد والمنع والاكتشافات والاستجابة، أي ربط جميع شبكات الأمن

الالكتروني للمراقبة والإشراف، وأن تصبح المخابرات الأمريكية ومجلس الأمن القومي متحدين في هدف مشترك مع مكتب التحقيقات الفيدرالية.

3- **بريطانيا:** المركز القومي للأمن السيبراني (National Cyber Security Centre) (NCSC): هو منظمة تابعة لحكومة المملكة المتحدة تقدم المشورة والدعم للقطاعين العام والخاص في كيفية تجنب تهديدات أمن الحاسوب. يقع مقرها الرئيسي في لندن، وبدأ تشغيله في أكتوبر 2016م، ومنظمتها الأم هي مكاتب الاتصالات الحكومية البريطانية مقر الاتصالات الحكومية (جي إتش سي كيو)، في إطار الخطة الخمسية الجديدة التي كشفتها بريطانيا في العام 2016م، وخصصت لها (1.9) مليار جنيه إسترليني (2.36) مليار دولار.

ثانياً : المراكز العربية

1- **المملكة الأردنية الهاشمية:** بتاريخ 3 شباط 2019م تم إنشاء أكاديمية كادبي للأمن السيبراني والتي تقدم خدمات الأمن السيبراني للمؤسسات الوطنية المعنية كافة، وتعتبر أكاديمية كادبي للأمن السيبراني، هي الجهة المؤهلة للتدريب في مجال الأمن السيبراني بالمملكة، وتجدر الإشارة إلى أن مجلس النواب الأردني قد أقر بأغلبيته في شهر 7 من العام 2019م، قانون الأمن السيبراني

"مكافحـة الهجـمات الالكترونيـة"، ووافـق المجلـس في هـذا القـانون الجديـد عـلى تأسـيس جسـمين جديـدين في هيكـل الحكومـة وهـما المجلس الوطني للأمن السيبراني والمركز الوطني للأمن السيبراني، ويتـيح هذا القانون تأسيس شركات أو مؤسسات خاصة تقدم الأنشطة الفنيـة والإدارية والاستشارية في مجال الأمن السيبراني بما فيها خدمات التقييم الأمني والمراقبة والتدقيق والخدمات الاستشارية.

2- **دولة الإمارات العربية المتحدة:** في العام 2007م أنشـأت هيئـة تنظـيم الاتصالات بدولة الإمـارات العربيـة المتحـدة مركـز الاسـتجابة لطـوارئ الحاسـب الآلي (Computer Emergency Response Centre Team(ae CERT))، لتحسـين معـايير وممارسـات أمـن المعلومـات وحمايـة البنيـة التحتيـة لتقنيـة المعلومـات مـن مخـاطر اختراقـات الإنترنت.

3- **مملكة البحـرين:** في 4 نـوفمبر 2012م قامـت "تحـديث للاستشـارات" (Reload Consulting Services) ، وهـي شركـة خاصـة مقرهـا البحرين بتأسيس مركز الاستجابة لطـوارئ الحاسـب الآلي (CERT) في مملكة البحرين.

4- **المملكة العربية السعودية:** المركز الوطني الإرشـادي لأمـن المعلومـات: فريـق الاستجابة لطوارئ الحاسب الآلي(Saudi Arabia Computer Emergency Response Team(CERT-SA))، تـم إنشـاء هـذا المركز بواسـطة هيئـة الاتصـالات وتقنيـة المعلومـات السـعودية (Communication and

(Information Technology Commission، ويهدف للكشف عن التهديدات والمخاطر، ومنع الاختراقات والانتهاك للأمن السيبراني والتنسيق والاستجابة للمعلومات عن حوادث الأمن السيبراني على مستوى المملكة، وفي شهر 3 من العام 2018م، صدر قرار رئيس مجلس إدارة الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، بإنشاء كلية الأمير محمد بن سلمان للأمن السيبراني والذكاء الاصطناعي والتقنيات المتقدمة، كما يعتبر مركز الأمن السيبرانى، بجامعة الأمير محمد بن فهد في السعودية مركز معتمد للتدريب بمنطقة الشرق الأوسط.

5- **سلطنة عمان:** في شهر 4 من العام 2010م افتتح المركز الوطني للسلامة المعلوماتية (National Information Safety Oman Center)، وتم في هذا المركز إنشاء فريق الاستجابة لطوارئ الحاسب الآلي(Computer Emergency Response (Team) (CERT ويتبع لهيئة تقنية المعلومات.

6- **دولة قطر**: فريق الاستجابة لطوارئ الحاسب الآلي القطري:(Qatar (Cybercrime Emergency Response Team (Q-CERT) في شهر 12 من العام 2005م تم إنشاء (المركز الوطني لأمن المعلومات(National Information Security Center) بواسطة المجلس الأعلى لهيئة تقنية المعلومات والاتصالات القطرية(ict . QATAR

7- **المركـز العـربي الإقليمـي للأمـن السـيبراني (Arab Area Cyber Security Regional Center) (ITU-ARCC)** : تـم تأسيسـه في ديسمبر 2012م من قبـل الاتحـاد الـدولي للاتصـالات (ITU) وسـلطنة عمان ممثلة في وزارة التقنية والاتصالات مع رؤية لإنشاء بيئة أكثر أمناً وتعاونـاً في مجـال الأمـن السـيبراني في المنطقـة العربيـة، وتعزيـز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمـن في اسـتخدام تكنولوجيـا المعلومات والاتصالات في المنطقة، تماشياً مع أهـداف الأجنـدة العالميـة الأمن السيبراني للإتحاد الدولي للاتصالات.

وفي العديد من دول العالم تم إنشاء مراكز استجابة للطوارئ الحاسوبية ومنها إضافة إلى النماذج أعلاه (الولايـات المتحـدة الأمريكيـة أسـتراليا، النمسـا، البرازيل، تشيلي، الصين، فنلندا، هنغاريا، الهند، ايطاليا، كوريـا، ماليزيـا، اليابـان، هولندا، بولندا، سلوفينيا، تونس، السويد، سويسرا، تايلند) وغيرها من الدول.

الخاتمة

ما زال الأمن بمستوياته المختلفة هو ذلك المطلب لجميع الدول، فإذا تحقق الأمن للدولة كما يجب، حافظت الدولة على كينونتها وعززت من موقعها بين مصاف الدول، إذا تحقق الأمن، انخفضت الجريمة وتحقق الرفاه الاجتماعي وتقدمت الدولة، ومن المفاهيم التي ظهرت حديثاً وارتبطت بالأمن هي (الأمن السيبراني)، والذي أصبح مفهوماً كان لا بد أن تتعامل معه الدول كواقع، وفعلاً تسارعت الدول إلى استيعاب هذا الحدث العالمي في المجال المعلوماتي، وعرفت الدول أن السيبرانية ليست إيجابيات مطلقة للبشرية، بل أنها إذا استغلت من الأشخاص ذوي الأنفس المريضة ستنعكس بالضرر على الفرد والأسرة والمؤسسات والشركات والاقتصاد والدول والعالم أجمع، حيث ظهر الإرهاب السيبراني والجريمة السيبرانية، ونلاحظ أن الإرهاب هو خطر تواجهه الدول من فترة طويلة ومع ظهور السيبرانية استخدمت الجماعات الإرهابية والمتطرفة هذا الفضاء للقيام بأعمالها التخريبية ضد الدول وزعزعة أمن الدول والبشرية، كما ظهر أشخاص أو مجموعة يمتازون بخصائص معينة إلا وهم (المجرمون السيبرانيين)، والذين أضافوا إلى علم الجريمة (الجريمة السيبراني)، ولقد سارعت الدول منفردة أو بالتشارك مع غيرها بالتعاون إلى مواجهة خطر السيبارنية وتعزيز الأمن السيبراني بجميع السبل المتاحة، ومنها إنشاء المراكز المختصة في حالات الطوارئ وتطوير التشريعات والقوانين بما يتناسب مع هذه الثورة المعلوماتية، إضافة إلى تدريب الكوادر البشرية

لمواكبة هذا التطور، كما تشجع الدول مراكز الأبحاث والمؤسسات التعليمية على الدراسة والتعمق في الفضاء السيبراني ونلاحظ أن جامعات عديدة غربية وعربية بدأت بتدريس مواضيع الأمن السيبراني، وعليه فالسيبرانية أخذت اهتمام الجميع قانونيين وتقنيين وسياسيين وأمنيين، ذلك أنها تعنيهم بشكل أو بآخر ويتوقع أن تزداد الدراسات والأبحاث والاهتمام خلال السنوات القادمة أكثر في هذا المجال. إن هذا الكتاب هو مدخل تعريفي لهذا الفضاء بجوانبه المختلفة، ورغم الجهد الذي بذله الباحث إلا أن السيبرانية مجال لا تغطيه عشرات الكتب، ويأمل المؤلف أن يكون هذا الكتاب تأسيساً وقاعدة لجهد آخر في مجال السيبرانية.

المصطلحات

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
1	اتصال/ مكالمة	Call
2	اتصالات	Communication
3	إجراءات التوثيق المحكمة	Verification procedures
4	أداة التوقيع الإلكتروني	e-signature tool
5	الإرهاب السيبراني	Cyberterrorism
6	إلكتروني (ة)	Electronic
7	اختراق	Hacking
8	انتهاك حقوق الملكية الفكرية	Copyright infringement
9	برامج التجسس	Spyware
10	برنامج الحاسوب	Computer software
11	برنامج الخصوصية الجيدة	Pretty good privacy
12	بروتوكول الإنترنت	Internet protocol
13	بيانات	Data
14	بيانات شخصية	Personal data
15	بيانات شخصية حساسة	Sensitive personal data
16	بيانات الموقع	Location data
17	تبادل البيانات الإلكترونية	Electronic data exchange
18	تجارة إلكترونية	Electronic commerce

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
19	تحويل إلكتروني للأموال	e-payment
20	الانتحال أو انتحال الصفة	Spoofing or phishing
21	تزوير معلوماتي	Computer-related forgery
22	تشفير	Encryption
23	توقيع إلكتروني	Electronic signature
24	حاسوب	Computer
25	جرائم الاستغلال الجنسي للقاصرين	Sexual abuse of minors
26	جرم الاحتيال أو الغش بوسيلة معلوماتية	Digital fraud or cyber fraud
27	جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية	Cyber embezzlement
28	جرم الإخفاق في الإبلاغ أو الإبلاغ الخاطئ عن جرائم المعلوماتية	Failing to report or bad reporting of a cyber crime
29	جرم الإرهاب بوسيلة معلوماتية	Cyber terrorism
30	جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها	Viewingand/or disseminating secret or sensitive data

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
31	جرم التحرش الجنسي بالقاصرين بوسيلة معلوماتية	Cyber sexual harassment against minors
32	جرم التحريض على القتل بوسيلة معلوماتية	Inciting to commit murder in a digital way
33	جرم التزود أو تزويد الغير بمواد إباحية لقاصرين بواسطة نظام معلوماتي	Procuring child pornography through a computer system for oneself or for another person
34	جرم التعرض للبيانات المعلوماتية	Data interference
35	جرم التنصت أو التقاط أو اعتراض الرسائل	Messages or communication
36	جرم الحصول بوسيلة معلوماتية على معلومات سرية تخص الدولة	Obtaining secre governmental data in a digital way
37	جرم العبث بالأدلة القضائية المعلوماتية	Cyber tampering with judicial evidence
38	جرم إساءة استعمال الأجهزة أو البرامج المعلوماتية	Misuse of computers and software
39	جرم استعمال بطاقة مصرفية	Use of forged credit card

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
	مقلدة	
40	جرم اعتراض بيانات معلوماتية	Digital data interception
41	جرم إفشاء معلومات ذات طابع شخصي	Dissemination of personal data
42	جرم بث بيانات تهدد الأمن والسلامة العامة بوسيلة معلوماتية	Digitally transmitting information that threatens public safety or national security
43	جرم ترويج المواد المخدرة على الإنترنت	Drug dealing online
44	جرم تزوير النقود الإلكترونية	Cyber money forgery
45	جرم تسهيل وتشجيع المقامرة على الانترنت	Facilitating and encouraging online gambling
46	جرم تعطيل الأعمال الحكومية بوسيلة معلوماتية	Cyber interference in government's activities
47	جرم تقليد إمضاء المؤلف أو ختمه	Forging author's signature or seal
48	جرم تقليد بطاقة مصرفية	Credit card counterfeiting
49	جرم تملك وإدارة مشروع	Owning and operating a gamblig business online

المصطلح باللغة الانجليزية	المصطلح باللغة العربية	الرقم
	مقامرة على الانترنت	
Cyber crime	جريمة سيبرانية	50
Firewall	جدار حماية	51
Computer server	حاسوب مخدم	52
Trojan horse	حصان طروادة	53
Copyright	حقوق النسخ والتأليف	54
Web server	خادم صفحات الويب	55
Electronic service	خدمة إلكترونية	56
Illegal access	دخول غير مشروع	57
Electronic platform	منصة إلكترونية	58
e-payment	دفع إلكتروني	59
Worm	دودة	60
Email bomb	رسالة إلكترونية قنبلة	61
Data message or email	رسالة إلكترونية أو بريد الكتروني	62
Data subject	شخص موضوع البيانات (صاحب البيانات)	63
Digital certificate	شهادة مصادقة الكترونية	64
Web page , website	صفحة الويب أو موقع الويب	65

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
	أو موقع الإنترنت	
66	تزييف	Pharming
67	فيروس	Virus
68	قاصر	Minor
69	قاعدة البيانات	Database
70	شيفرة خبيث	Malicious code
71	متلقي البيانات	Recipient
72	مجتمع المعلومات	Information society
73	محترف	Professional
74	مراسلة إلكترونية	Electronic communication
75	مزود خدمة الإنترنت	Internet service provider
76	مساعدة أو تحريض بوسيلة الكترونية على ارتكاب جرائم ضد الإنسانية	Inciting or assisting in committing crimes against humanity online
77	مضايقة أو ملاحقة السيبرانية	Cyber stalking
78	معالج البيانات	Data processor
79	معالجة البيانات الشخصية	Processing of personal data
80	معاملات إلكترونية	Electronic transactions
81	عنوان بروتوكول الانترنت	Ip address

الرقم	المصطلح باللغة العربية	المصطلح باللغة الانجليزية
82	معلومات إلكترونية	Electronic information
83	ملف بيانات ذات طابع شخصي	Personal data file
84	نظام معالجة البيانات	Data Processing system
85	نقل البيانات	Data transfer
86	نقل المعلومات للجمهور بوسيلة إلكترونية	Electronic data transfer to the public
87	نقود إلكترونية	e-money
88	وسائل الاتصال عن بعد	Means of distance communication
89	وسائل اتصال إلكترونية	Electronic communication means
90	وسائل تشفير المعلومات	Encryption methods
91	وسيط إلكتروني	Electronic intermediary

الملاحق

الملحق رقم (1)

الاتفاقية العربية لمكافحة تقنية المعلومات

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الديباجة

إن الدول العربية الموقعة:

رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها.

واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات.

وأخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة.

والتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها.

فقد اتفقت على ما يلي:

الفصل الأول - أحكام عامة

المادة الأولى: الهدف من الاتفاقية:

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

المادة الثانية: المصطلحات:

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1. **تقنية المعلومات:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزونة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لا سلكياً في نظام أو شبكة..
2. **مزود الخدمة:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.
3. **البيانات:** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها .
4. **البرنامج المعلوماتي:** مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما .
5. **النظام المعلوماتي:** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات .
6. **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها .

7. **الموقع:** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد .

8. **الالتقاط:** مشاهدة البيانات أو المعلومات أو الحصول عليها .

9. **معلومات المشترك:** أية معلومات موجودة لدى مزود الخدمة المدنية والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ- نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة .

ب- هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.

ج- أية معلومات أخرى عن موضع تركيب معدات الاتصال بناء على اتفاق الخدمة.

المادة الثالثة: مجالات التطبيق:

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية:

1. ارتكبت في أكثر من دولة.

2. ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.

3. ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.
4. ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

المادة الرابعة: صون السيادة:

1. تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.
2. ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

الفصل الثاني - التجريم

المادة الخامسة: التجريم: تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية .

المادة السادسة: جريمة الدخول غير المشروع:

1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به .

2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبينات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين .

ب- الحصول على معلومات حكومية سرية .

المادة السابعة: جريمة الاعتراض غير المشروع:

الاعتراض المعتمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بينات تقنية المعلومات .

المادة الثامنة: الاعتداء على سلامة البيانات:

1. تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق .
2. للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم .

المادة التاسعة: جريمة إساءة استخدام وسائل تقنية المعلومات:

1. إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ- أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة .

ب- كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد

استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2. حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة .

المادة العاشرة: جريمة التزوير:

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقية في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبينات صحيحة .

المادة الحادية عشرة: جريمة الاحتيال:

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

1. إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات .
2. التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها .
3. تعطيل الأجهزة والبرامج والمواقع الإلكترونية .

المادة الثانية عشرة: جريمة الإباحية:

1. إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات .
2. تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر .

3. يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات .

المادة الثالثة عشرة: الجرائم الأخرى المرتبطة بالإباحية:

المقامرة والاستغلال الجنسي .

المادة الرابعة عشرة:جريمة الاعتداء على حرمة الحياة الخاصة:

الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات .

المادة الخامسة عشرة: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1. نشر أفكار ومبادئ جماعات إرهابية والدعوة لها .
2. تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية .
3. نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية .
4. نشر النعرات والفتن والاعتداء على الأديان والمعتقدات .

المادة السادسة عشرة: الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:

1. القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.
2. الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها .

3. الاتجار بالأشخاص .

4. الاتجار بالأعضاء البشرية .

5. الاتجار غير المشروع بالأسلحة .

المادة السابعة عشرة: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة:

انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي .

المادة الثامنة عشرة: الاستخدام غير المشروع لأدوات الدفع الإلكترونية:

1. كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت .
2. كل من استولى على بيانات أي أداة من أدوات واستعملها أو قدمها للغير أو سهل للغير الحصول عليها .
3. كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع .
4. كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك .

المادة التاسعة عشرة: الشروع والاشتراك في ارتكاب الجرائم:

1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف .
2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية .
3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً .

المادة العشرون: المسؤولية الجنائية للأشخاص الطبيعية والمعنوية:

تلتزم كل دولة طرف مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً .

المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات .

المادة الثانية والعشرون: نطاق تطبيق الأحكام الإجرائية:

1- تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.

2- مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على:

أ- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية .

ب- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات .

ج- جميع الأدلة عن الجرائم بشكل إلكتروني .

3- أ- يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة الثلاثين، وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادة التاسعة العشرين .

ب- كما يجوز للدولة الطرف أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية غير

قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي ثبت بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية:

- يتم تشغيلها لصالح مجموعة مفغلقة من المستخدمين .
- لا تستخدم شبكات اتصال عامة وليست مرتبطة بتقنية معلومات أخرى سواء كانت عامة أو خاصة .

وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين التاسعة والعشرين والثلاثين .

المادة الثالثة والعشرون: التحفظ العاجل على البيانات المخزنة في تقنية المعلومات:

1. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل .
2. تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها (90) يوماً قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي .

3. تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي .

المادة الرابعة والعشرون: التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين:

تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل:

1. ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات .
2. ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات .

المادة الخامسة والعشرون: أمر تسليم المعلومات:

تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى:

1. أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات .

2. أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته .

المادة السادسة والعشرون: تفتيش المعلومات المخزنة:

-1 تلتزم كل دولة طرف يتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ- تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها .

ب- بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه .

-2 تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة (1- أ)، إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في

التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

المادة السابعة والعشرون: ضبط المعلومات المخزنة:

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (1) من المادة السادسة والعشرين من هذه الاتفاقية .

هذه الإجراءات تشمل صلاحيات:

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات .

ب- عمل نسخة معلومات تقنية المعلومات والاحتفاظ بها .

ج- الحفاظ على سلامة معلومات تقنية المعلومات المخزنة .

د- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها .

3- تلتزم كل طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين (1 و 2) من المادة السادسة والعشرين من هذه الاتفاقية .

المادة الثامنة والعشرون: الجمع الفوري لمعلومات تتبع المستخدمين:

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من:

أ- جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف .

ب- إلزام مزود الخدمة ضمن اختصاصه الفني بأن:

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.
- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تثبت بواسطة تقنية المعلومات.

2- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1- أ)، فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

4- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

المادة التاسعة والعشرون: اعتراض معلومات المحتوى:

1- تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

أ- الجمع أو التسجيل من خلال الوسائل الفنية على إقليم تلك الدولة الطرف.

ب- التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي ثبت بواسطة تقنية معلومات .

2- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة (1- أ)، فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم .

4- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

المادة الثلاثون: الاختصاص:

1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت:

أ- في إقليم الدولة الطرف .

ب- على متن سفينة تحمل علم الدولة الطرف .

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف .

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكبها أو إذ ارتكبت خارج منطقة الاختصاص القضائي لأية دولة .

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة .

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم .

3- إذا ادعت أكثر من دولة بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها

أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليم ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا تحددت الظروف فتقدم الدولة الأسبق في طلب التسليم .

المادة الحادية والثلاثون: تسليم المجرمين:

1- أ- هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب- إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق .

2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3- إذ قامت دولة طرف ما بجعل تسليم المجرمين مشروطاً بوجود معاهدة، وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم، فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة .

4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول .

5- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين .

6- يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين، وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة مصحوباً بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم .

7- أ- تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس

وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

ب- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف، وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائماً .

المادة الثانية والثلاثون: المساعدة المتبادلة:

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم..

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين .

3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الإلكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير)، وتأكيد الإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منه المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات .

4- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة، بما في ذلك الأسس التي يمكن للدولة المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية .

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فعن هذا الشرك يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة، وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف .

المادة الثالثة والثلاثون: المعلومات العرضية المتلقاة:

1- يجوز لأي دولة طرف - ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها، من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات، يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف .

2- قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات، وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين .

المادة الرابعة والثلاثون: الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة:

1- تطبق بنود الفقرات (2- 9) من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة والمطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي .

2- أ- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.

ب- على السلطات المركزية أن تتصل ببعضها مباشرة.

ج- على كل دولة طرف- وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة.

د- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصي الموجودة في السجل صحيحة دائما .

3- يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة .

4- يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها .

5- قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذ سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية .

6- تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب، وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير .

7- يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر لكافي لتنفيذ الطلب، وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب .

8- أ- في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة الوقت من

السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.

ب- يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول.

ج- حيثما يتم تقديم طلب حسب الفقرة (أ) ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك .

د- إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري، يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

هـ- يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية .

المادة الخامسة والثلاثون: رفض المساعدة:

يجوز للدولة الطرف المطلوب منها المساعدة- بالإضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثين الفقرة (4) أن ترفض المساعدة إذا:

1. كان الطلب متعلقاً بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية.
2. اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادته أو أمنه أو نظامه أو مصالحه الأساسية.

المادة السادسة والثلاثون: السرية وحدود الاستخدام:

-1 عندما لا يكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع الساري بين الدول الأطراف الطالبة والمطلوب منها، فيجب تطبيق بنود هذه المادة ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق أي من فقرات هذه المادة أو كلها.

-2 يجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب بشرط:

أ- الحفاظ على عنصر السرية للدولة الطرف الطالبة للمساعدة ولا يتم الالتزام بالطلب في غياب هذا العنصر .

ب- عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب .

-3 إذا لم تستطع الدولة الطرف الطالبة الالتزام بالشرط الوارد في الفقرة (2) فيجب عليها إعلام الدولة الطرف الأخرى والتي ستقرر بعدها مدى إمكانية توفير المعلومات، وإذا قبلت الدولة الطرف الطالبة بهذا الشرط فهو ملزم لها.

4- أي دولة طرف توفر المعلومات أو المواد بحسب الشرط في الفقرة (2) لتوفير المعلومات يجوز لها أن تطلب من الدولة الطرف الأخرى أن تبرر استخدام المعلومات أو المواد.

المادة السابعة والثلاثون: الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات:

1- لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

2- يجب أن يحدد طلب الحفظ حسب الفقرة (1) ما يلي:

أ- السلطة التي تطلب الحفظ .

ب- الجريمة موضوع التحقيق وملخصا للوقائع .

ج- معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة .

د- أية معلومة متوفرة لتحديد المسؤول عن المعلومات المخزنة أو موقع تقنية المعلومات .

هـ- موجبات طلب الحفظ .

و- رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصول أو الضبط أو تأمين أو كشف معلومات تقنية المعلومات المخزنة .

3- عند استلام إحدى الدول الأطراف من دولة أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب، فلا يشترط وجود ازدواجية التجريم للقيام بالحفظ.

4- أي دولة طرف تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الاتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذ كان هناك سبب للاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

5- بالإضافة لذلك، يمكن رفض طلب الحفظ إذا:

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- اعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها .

6- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيق الدولة الطرف الطالبة لها أو سلاكتها، فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب .

7- أي حفظ ناجم عن الاستجابة للطلب المذكور في الفقرة (1) يجب أن يكون لفترة لا تقل عن (60) يوما من أجل تمكين الدولة الطرف الطالبة من تسليم البحث أو الوصول أو الضبط أو التأمين أو

الكشف للمعلومات. وبعد استلام مثل هـذا الطلـب يجـب الاسـتمرار بحفظ المعلومات حسب القرار الخاص بالطلب .

المـادة الثامنـة والثلاثـون: الكشـف العاجـل لمعلومـات تتبـع المسـتخدمين المحفوظة:

1- حيثما تكتشف الدولة الطرف المطلوب منها - في سياق تنفيذ الطلـب حسب المـادة السـابعة والثلاثـين لحفـظ معلومـات تتبـع المسـتخدمين الخاصة باتصالات معينة - بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال، فيجـب عـلى الدولـة الطـرف المطلـوب منهـا أن تكشـف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبـع المسـتخدمين مـن أجل تحديد مزود الخدمة ومسار بث الاتصالات .

2- يمكن تعليق كشف معلومات تتبع المستخدمين حسب الفقرة (1) إذا:

أ- تعلق الطلب بجريمـة تعتبرهـا الدولـة الطـرف المطلـوب منهـا جريمة سياسية..

ب- اعتبرت الدولة الطـرف المطلـوب منهـا بـأن تنفيـذ الطلـب قـد يهدد سلامتها أو أمنها أو نظامها أو مصالحها .

المادة التاسعة والثلاثون: التعـاون والمسـاعدة الثنائيـة المتعلقـة بالوصـول إلى معلومات تقنية المعلومات المخزنة:

1. يجوز لأي دولة طرف أن تطلب مـن دولـة أخـرى البحـث أو الوصـول أو الضبط أو التأمين أو الكشـف لمعلومـات المخزنـة والواقعـة ضـمن

أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.

2. تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.

3. تم الإجابة على الطلب على أساس عاجل المعلومات ذات العلاقة عرضه للفقدان أو التعديل.

المادة الأربعون: الوصول إلى معلومات تقنية المعلومات عبر الحدود:

يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى:

1. أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات.

2. أن تصل أو تستقبل - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى، وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

المادة الحادية والأربعون: التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:

1. على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينة في أقاليمها والتي تثبت بواسطة تقنية المعلومات.

2. على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المتخدمين لمثليها من القضايا الداخلية .

المادة الثانية والأربعون: التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية .

المادة الثالثة والأربعون: جهاز متخصص:

1- تكفل كل دولة طرف، وفقا للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ:

أ- توفير المشورة الفنية .

ب- حفظ المعلومات استنادا للمادتين السابعة والثلاثين والثامنة والثلاثين .

ج- جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين .

2- أ- يجب أن يكون ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة .

ب- إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءاً من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية، فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة .

3- على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه .

الفصل الخامس - أحكام ختامية

1. تعمل الجهات المختصة لدى الدول الأطراف على اتخاذ الإجراءات الداخلية اللازمة لوضع هذه الاتفاقية موضع التنفيذ.

2. تكون هذه الاتفاقية محلا للتصديق عليها أو قبولها أو إقرارها من الدول الموقعة، وتودع وثائق التصديق أو القبول أو الإقرار لدى الأمانة العامة لجامعة الدول العربية في موعد أقصاه ثلاثون يوما من تاريخ التصديق أو القبول أو الإقرار، وعلى الأمانة العامة إبلا سائر الدول الأعضاء والأمانة العامة لمجلس وزراء الداخلية العرب بكل إيداع لتلك الوثائق وتاريخه.

3. تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية.
4. يجوز لأية دولة من دول الجامعة العربية غير الموقعة على هذه الاتفاقية أن تنضم إليها، وتعتبر الدولة طرفاً في هذه الاتفاقية بمجرد إيداع وثيقة التصديق أو القبول أو الإقرار أولاً، وتعتبر الدولة طرفاً الانضمام لدى الأمانة العامة لجامعة الدول العربية، ومضي ثلاثين يوما على تاريخ الإيداع.
5. مع مراعاة ما نصت عليه الفقرة (3) من المادة التاسعة عشرة، إذا تعارضت أحكام هذه الاتفاقية مع أحكام أية اتفاقية خاصة سابقة يطبق النص الأكثر تحقيقاً لمكافحة جرائم تقنية المعلومات.
6. لا يجوز لأية دولة من الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو خروج على أهدافها.
7. يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية وتحيله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف، ويصبح هذا التعديل نافذاً بعد مضي ثلاثين يوماً من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول أطراف لدى الأمانة العامة لجامعة الدول العربية.
8. يمكن لأية دولة طرف أن تنسحب من هذه الاتفاقية بناء على طلب كتابي ترسله إلى الأمين العام لجامعة الدول العربية. ويرتب

الانسحاب أثره بعد مضي ستة أشهر من تاريخ إرسال الطلب إلى الأمين العام لجامعة الدول العربية .

خاتمة

حررت هذه الاتفاقية باللغة العربية بمدينة القاهرة في جمهورية مصر العربية في 1432/1/15هـ الموافق 2010/12/21م، من أصل واحد مودع بالأمانة العامة لجامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف. وإثباتا لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب ، بتوقيع هذه الاتفاقية، نيابة عن دولهم.

قائمة الدول العربية الموقعة والمصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

1. وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 15/ 1/ 1432هـ الموافق 21/ 12/ 2010م.
2. تسري هذه الاتفاقية بعد مضي ثلاثين يوماً من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية بموجب الفقرة (3) من الأحكام الختامة للاتفاقية.

الدولة	تاريخ التوقيع	تاريخ التصديق أو القبول أو الإقرار
المملكة الأردنية الهاشمية	2010/12/21م	2013/1/8
دولة الإمارات العربية المتحدة	2010/12/21م	2011/9/21م
مملكة البحرين	2010/12/21م	-
الجمهورية التونسية	2010/12/21م	-
الجمهورية الجزائرية الديمقراطية الشعبية	2010/12/21م	-
جمهورية جيبوتي		-
المملكة العربية السعودية	2010/12/21م	-
جمهورية السودان	2010/12/21م	2013/7/15
الجمهورية العربية السورية	2010/12/21م	-
جمهورية الصومال		-
جمهورية العراق	2010/12/21م	-
سلطنة عمان	2010/12/21م	-

الدولة	تاريخ التوقيع	تاريخ التصديق أو القبول أو الإقرار
دولة فلسطين	2010/12/21م	2012/5/24م
جمهورية القمر المتحدة		-
دولة الكويت	2010/12/21م	2013/9/5
الجمهورية اللبنانية		-
دولة ليبيا	2010/12/21م	-
جمهورية مصر العربية	2010/12/21م	-
المملكة المغربية	2010/12/21م	-
الجمهورية الإسلامية الموريتانية	2010/12/21م	-
الجمهورية اليمنية	2010/12/21م	-

ملحق رقم (2)

الاتفاقية المتعلقة بالجريمة الإلكترونية بودابست 2001م

الديباجة

إن الدول الأعضاء في مجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية؛ إذ تأخذ في الاعتبار أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛ واعترافاً منها بقيمة تعزيز التعاون مع الدول الأخرى الأطراف في هذه الاتفاقية؛ واقتناعاً منها بالحاجة إلى إتباع سياسة جنائية مشتركة، كمسألة ذات أولوية، بهدف حماية المجتمع من الجريمة الإلكترونية، من خلال تبني تشريع ملائم ودعم التعاون الدولي، من بين أمور أخرى؛ وإدراكاً منها بعمق التغييرات التي أحدثتها الرقمنة والالتقائية والعولمة المتواصلة لشبكات الكومبيوتر؛ وإذ يساورها القلق بشأن مخاطر إمكانية استخدام شبكات الكومبيوتر والمعلومات الإلكترونية أيضا لارتكاب جرائم جنائية، وأن الأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات؛ واعترافاً منها بالحاجة إلى التعاون بين الدول والقطاع الخاص في مجال مكافحة الجريمة الإلكترونية، والحاجة إلى حماية المصالح المشروعة عند استخدام وتطوير تكنولوجيا المعلومات؛ وإيماناً منها بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم تعزيز التعاون الدولي في المسائل الجنائية وتسريع وتيرته وتوظيفه بشكل جيد؛ واقتناعاً منها بأن هذه الاتفاقية ضرورية لردع الأعمال الموجهة ضد سرية وسلامة

وتوافر نظم الكومبيوتر، والشبكات والبيانات بالإضافة إلى إساءة استخدام هذه النظم والشبكات والبيانات، وذلك بالتنصيص على تجريم سلوكيات من هذا القبيل، كما هو مبين في هذه الاتفاقية واعتماد الصلاحيات الكافية من أجل مكافحة فعالة لمثل هذه الجرائم الجنائية من خلال تيسير كشفها، والتحقيق بشأنها، ومقاضاتها على المستويين الوطني والدولي على حد سواء، وكذلك عن طريق توفير ترتيبات من أجل تحقيق تعاون دولي سريع وموثوق؛ وحرصاً منها على ضرورة تأمين التوازن الملائم بين المصالح المتصلة بإنفاذ القانون من جهة واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام 1950م بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966م المتعلق بالحقوق المدنية والسياسية، وغيرها من المعاهدات الدولية بشأن حقوق الإنسان السارية والتي تؤكد حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير، بما في ذلك حرية البحث عن مختلف أنواع المعلومات والأفكار وتلقيها ونقلها بغض النظر عن الحدود، علاوة على الحقوق المتعلقة باحترام الخصوصية؛ وحرصاً منها كذلك على الحق في حماية البيانات الشخصية، الذي تخوله على سبيل المثال اتفاقية مجلس أوروبا لعام 1981م بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛ وإذ تأخذ في الاعتبار اتفاقية الأمم المتحدة لعام 1989م بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام 1999م بشأن أسوأ صور عمل الأطفال؛ وإذ تأخذ بعين الاعتبار اتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي، وكذلك المعاهدات

المماثلة القائمة بين الدول الأعضاء في مجلس أوروبا وغيرها من الدول، وتؤكد على أن الاتفاقية الحالية ترمي إلى استكمال تلك الاتفاقيات بغية تعزيز فعالية التحقيقات والإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بنظم وبيانات الكومبيوتر، والتمكين من جمع الأدلة في الجرائم الجنائية ذات الطابع الإلكتروني؛ وإذ ترحب بالتطورات الأخيرة التي تعزز التفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية، بما في ذلك الإجراء الذي اتخذته منظمة الأمم المتحدة، ومنظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي ومجموعة الثمانية؛ وإذ تذكر بتوصيات لجنة الوزراء رقم (85/10) بشأن التطبيق العملي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية، والتوصية رقم (88/2) بشأن القرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة، والتوصية رقم (87/15) التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم (95/4) بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات مع إشارة خاصة إلى الخدمات الهاتفية، بالإضافة إلى التوصية رقم (89/9) بشأن الجرائم ذات الصلة بالكمبيوتر التي توفر مبادئ توجيهية للهيئات التشريعية الوطنية بشأن تعريف بعض جرائم الكومبيوتر، والتوصية رقم (95/13) بشأن المشاكل التي يطرحها قانون الإجراءات الجنائية علاقة بتكنولوجيا المعلومات؛ ومراعاة للقرار رقم (1) الذي تبناه وزراء العدل الأوروبيون في مؤتمرهم الواحد والعشرين (براغ، في 10 و11 يونيو/حزيران 1997م) والذي أوصى لجنة الوزراء بدعم الجهود التي تبذلها

اللجنـة الأوروبيـة المعنيـة بمشـاكل الإجـرام (CDPC) في مجـال الجريمـة الإلكترونية بغية تقريب أحكام القوانين الجنائية الوطنيـة مـن بعضـها الـبعض، وتمكين استخدام الوسـائل الفعالـة لإجـراء التحقيقـات في مثـل هـذه الجـرائم، بالإضافة إلى القرار رقم (3) المعتمد خلال المؤتمر الثاني لوزراء العدل الأوروبيين (لندن، 8 و9 يونيو/ حزيـران 2000م) والـذي شـجع الأطـراف المتفاوضـة عـلى مواصلة جهودهم بغرض إيجـاد حلـول ملائمـة لتمكـين أكـبر عـدد ممكـن مـن الـدول أن تصـبح أطرافـاً في الاتفاقيـة، وأقـر بالحاجـة إلى نظـام سريـع وفعـال للتعـاون الـدولي يأخـذ بعـين الاعتبـار وكـما يجـب الشروط الخاصـة بمكافحـة الجريمـة الإلكترونيـة؛ وبـالنظر لخطـة العمـل التـي اعتمـدها رؤسـاء الـدول والحكومات الأعضاء في مجلس أوروبا بمناسبة انعقاد القمة الثانية (ستراسبورغ، 10 و11 أكتـوبر/ تشريـن الأول 1997م) بغيـة إيجـاد ردود مشـتركة لتطـور تكنولوجيات المعلومات الحديثة وفقاً لمعايير وقيم مجلس أوروبا؛ **اتفقت عـلى ما يلي:**

الباب الأول- استخدام المصطلحات

المادة 1- التعريفات

لأغراض هذه الاتفاقية:

أ. يُقصد بـ "منظومة الكمبيوتر" أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقاً لبرنامج، بالمعالجة الآلية للبيانات.

ب. يُقصد بـ "بيانات الكمبيوتر" أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكمبيوتر، بما في ذلك برنامج مناسب يساعد نظام كمبيوتر في أداء وظيفة معينة.

ج. يُقصد بـ " مُقدم الخدمة:

1- أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكمبيوتر.

2- أي كيان آخر يقوم بمعالجة بيانات الكمبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

د. يُقصد بـ" بيانات حركة الاتصالات" أي بيانات كمبيوتر متعلقة باتصال عن طريق نظام الكمبيوتر والتي تنشأ عن نظام كمبيوتر يشكل جزءاً في سلسلة الاتصالات، توضح المنشأ، والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية.

الباب الثاني: التدابير الواجب اتخاذها على الصعيد الوطني

القسم الأول: القانون الجنائي الموضوعي

الفصل الأول: الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر

المادة 2- النفاذ غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِية الحصول على بيانات الكمبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر.

المادة 3 - الاعتراض غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكمبيوتر إلى أو من أو داخل نظام كمبيوتر، بما في ذلك الانبعاثات

الكهرومغناطيسية الصادرة عن نظام كمبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِيَّة غير صادقة أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر.

المادة 4 - التدخل في البيانات

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.

2- يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة (1) في ضرر جسيم.

المادة 5 - التدخل في النظام

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكمبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها.

المادة 6 - إساءة استخدام الأجهزة

-1 تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق.

أ. عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى:

1. جهاز، بما في ذلك برنامج كمبيوتر، تم تصميمه أو ملاءمته مبدئياً، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من (2) إلى (5).

2. كلمة سر خاصة بكمبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من (2) إلى (5).

ب. حيازة إحدى المواد المشار إليها في الفقرة أ (1) أو (2) أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من (2) إلى (5). ويجوز للدولة الطرف أن تشترط بموجب القانون أن تكون حيازة عدد من هذه المواد سابقة لإلحاق المسؤولية الجنائية.

3. لا يجوز تُفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع، الشراء بغرض الاستخدام، الاستيراد،

التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها بالفقرة (1) من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من (2) إلى (5) من هذه الاتفاقية، بل بالأحرى للاستخدام المرخص لغرض اختبار أو حماية نظام الكمبيوتر.

4. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة (1) من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع، توزيع أو إتاحة هذه المواد المشار إليها في الفقرة (1- أ 2) من هذه المادة.

الفصل الثاني: الجرائم ذات الصلة بالكمبيوتر

المادة 7 - التزوير المرتبط بالكمبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: إدخال، تغيير، حذف أو إتلاف بيانات كمبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

المادة 8 - الاحتيال المرتبط بالكمبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ. أي إدخال، تغيير، حذف أو إتلاف لبيانات الكمبيوتر.

ب. أي تدخل في وظيفة نظام الكمبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق، على منفعة اقتصادية ذاتية أو لفائدة شخص آخر.

الفصل الثالث: الجرائم ذات الصلة بالمحتوى

المادة 9 - الجرائم ذات الصلة بمواد إباحية عن الأطفال

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق:

أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكمبيوتر.

ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكمبيوتر.

ج. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكمبيوتر.

د. الحصول على مواد إباحية عن الأطفال عبر نظام الكمبيوتر لصالح الشخص ذاته أو لفائدة الغير.

هـ حيازة مواد إباحية عن الأطفال داخل نظام الكمبيوتر أو على دعامة لتخزين بيانات الكمبيوتر.

2- لغرض الفقرة (1) أعلاه، تشمل عبارة "مواد إباحية عن الأطفال" المواد الإباحية التي تعرض بشكل مرئي:

أ. قاصر وهو يمارس سلوكاً جنسياً واضحاً.

ب. شخص يبدو قاصراً وهو يمارس سلوكاً جنسياً واضحاً.

ج. صور واقعية تظهر قاصراً وهو يمارس سلوكاً جنسيا واضحاً.

3- لغرض الفقرة (2) أعلاه ، يشمل مصطلح "قاصر" كافة الأشخاص دون سن الثامنة عشر. ويجوز لأي دولة طرف أن تشترط حداً عمرياً أدنى لا يقل عن سن السادسة عشر.

4- يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين "د" و "هـ" من الفقرة (1) والبندين "ب" ، "ج" من الفقرة (2).

الفصل الرابع: الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

المادة 10 - الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 يوليو/ تموز 1971م والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر.

2- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق ذات الصلة، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة الويبو بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر.

3- يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين (1) و (2) من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين (1) و (2) من هذه المادة.

الفصل الخامس: المسؤولية الإضافية والعقوبات

المادة 11 - المحاولة، والمساعدة والتحريض

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من (2) إلى (10) من هذه الاتفاقية، وذلك بِنية ارتكاب جريمة من هذا القبيل.

2- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: محاولة ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من (3 إلى 5، 7، 8 و) (1) (أ) و(ج) من هذه الاتفاقية.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة (2) من هذه المادة كلياً أو جزئياً.

المادة 12 - مسؤولية الشركات

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن الجرائم المنصوص عليها في هذه الاتفاقية التي تُرتكب لمصلحتها من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضواً في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قيادياً داخلها، وذلك بناء على:

أ. سلطة تمثيل الشخص الاعتباري.

ب. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري.

ج. سلطة ممارسة الرقابة لدى الشخص الاعتباري.

2- بالإضافة إلى الحالات المنصوص عليها مسبقا في الفقرة (1) من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان مساءلة الشخص الاعتباري في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة (1) في ارتكاب جريمة منصوص عليها وفقا لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

3- رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية، مدنية أو إدارية.

4- لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

المادة 13 - العقوبات والتدابير

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من (2) إلى (11) مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية.

2- تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقاً للمادة (12) وإخضاعهم لعقوبات أو تدابير فعالة، متناسبة ورادعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات المالية

القسم الثاني: القانون الإجرائي الفصل الأول: أحكام مشتركة

المادة 14 - نطاق الأحكام الإجرائية

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار السلطات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات والدعاوى الجنائية المحددة.

2- باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في المادة (21)، تطبق كل دولة طرف السلطات والإجراءات المشار إليها في الفقرة (1) من هذه المادة على:

أ. الجرائم الجنائية المقررة في المواد من (2) إلى (11) من هذه الاتفاقية.

ب. الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكمبيوتر.

ج. جمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني.

3- أ. يجوز لكل دولة طرف أن تحتفظ بالحق في تطبيق الإجراءات المشار إليها بالمادة (20) فقط على الجرائم أو أصناف الجرائم المحددة في التحفظ، شريطة ألا يكون نطاق هذه الجرائم أو أصناف الجرائم مقيداً بشكل أكبر من نطاق الجرائم التي تطبق عليها الإجراءات المشار إليها في المادة (21). ويتعين على كل دولة طرف النظر في تقييد هذا

التحفظ بشكل يمكّن من تطبيق التدبير المشار إليه في المادة (20) على أوسع نطاق.

ب. في حال تعذر على دولة طرف، بسبب قيود موجودة في تشريعاته السارية وقت التصديق على هذه الاتفاقية، تطبيق التدابير المشار إليها في المادتين 20 و21 على الاتصالات المنقولة داخل نظام الكومبيوتر لمزود الخدمة، عندما يكون ذلك النظام:

1. مشغلاً لفائدة مجموعة مغلقة من المستخدمين.

2. لا يستخدم شبكات الاتصالات العمومية، وغير متصل بأي نظام كمبيوتر آخر، سواء كان عاماً أو خاصاً.

فإنه يجوز لتلك الدولة الطرف الاحتفاظ بالحق في عدم تطبيق هذه التدابير على تلك الاتصالات. ويتعين على كل دولة طرف النظر في تقييد هذا التحفظ بشكل يمكّن من تطبيق التدبير المشار إليه في المادة (20) على أوسع نطاق.

المادة 15 - الشروط والضمانات

1- تسعى كل دولة طرف إلى ضمان خضوع وضع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذا القسم، للضمانات والشروط المنصوص عليها في قانونها الوطني، الذي ينبغي أن يوفر الحماية الملائمة لحقوق الإنسان والحريات، بما في ذلك

الحقوق الناشئة عن الالتزامات التي تعهدت بها بموجب اتفاقية مجلس أوروبا لعام 1950م الخاصة بحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966م الخاص بالحقوق المدنية والسياسية، وغيرها من الصكوك الدولية ذات الصلة بحقوق الإنسان، وأن يدمج مبدأ التناسب.

-2 تشمل هذه الشروط والضمانات، حسب الاقتضاء بالنظر لطبيعة الإجراءات أو السلطات المعنية، الإشراف القضائي أو بواسطة أي هيئة مستقلة أخرى، والأسس المبررة للتطبيق، وحدود نطاق تلك الإجراءات أو السلطات ومدتها، من بين أمور أخرى.

-3 بقدر ما يتفق مع المصلحة العامة، خاصة الإدارة السليمة للعدالة، يقوم كل طرف بتدارس تأثير السلطات والإجراءات الواردة في هذا القسم على حقوق الأغيار ومسؤولياتهم ومصالحهم المشروعة.

الفصل الثاني: التعجيل في حفظ بيانات الكمبيوتر المخزنة

المادة 16- التعجيل في حفظ بيانات الكمبيوتر المخزنة

-1 تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من الأمر أو الحصول على الحفظ المعجل لبيانات كمبيوتر محددة، بما في ذلك بيانات الحركة

المُخزنة بواسطة نظام الكمبيوتر، خاصة في حال وجود أسس للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل.

2- في حال تفعيل دولة طرف للفقرة (1) أعلاه عبر توجيه أمر إلى شخص من أجل حفظ بيانات كمبيوتر محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكمبيوتر المعنية والإبقاء على سلامتها لأطول مدة زمنية ضرورية على ألا تتجاوز تسعين يوماً، من أجل تمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف التنصيص على تجديد هذا الأمر لاحقاً.

3- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام القيِّم على حفظ بيانات الكمبيوتر أو أي شخص آخر عهدت له هذه المهمة، بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانونها الوطني.

4- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و 15).

المادة 17 - التعجيل في حفظ بيانات الكمبيوتر والكشف الجزئي عن بيانات الحركة

1- تعتمد كل دولة طرف، فيما يتعلق ببيانات الحركة الواجب حفظها بموجب المادة (16)، ما يلزم من تدابير تشريعية وغيرها من التدابير بغية:

أ. ضمان توفر إمكانية التعجيل في حفظ بيانات الحركة بصرف النظر عن مشاركة مزود خدمة واحد أو أكثر في عملية نقل هذا الاتصال.

ب. ضمان تعجيل الكشف للسلطة المختصة لدى الدولة الطرف، أو الشخص الذي تعينه تلك السلطة، عن القدر الكافي من بيانات الحركة من أجل تمكين الدولة الطرف من تحديد مزود الخدمة والمسار الذي تم من خلاله نقل الاتصال.

2- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و15).

الفصل الثالث: الأمر بإبراز البيانات

المادة 18 - الأمر بإبراز البيانات

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى:

أ.   أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر.

ب.   أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.

2-   تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و15).

3-   لغرض هذه المادة، يقصد بعبارة "معلومات عن المشترك" أي معلومات مدرجة في شكل بيانات الكمبيوتر أو في أي شكل آخر يحفظها مزود الخدمة والتي تتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

أ.   نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة.

ب.   هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة.

ج.   أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال والمتاحة بموجب اتفاق أو ترتيبات الخدمة.

الفصل الرابع: البحث عن بيانات الكمبيوتر المخزنة ومصادرتها

المادة 19 - البحث عن بيانات الكومبيوتر المخزنة ومصادرتها:

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من البحث عن أو النفاذ إلى:

أ. أي نظام كومبيوتر أو أي جزء منه وبيانات الكمبيوتر المخزنة فيه.

ب. أي دعامة تخزين بيانات الكمبيوتر يمكن أن تكون بيانات كمبيوتر مخزنة داخلها على أراضي تلك الدولة الطرف.

2- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان أنه في حال إنجاز سلطاتها لعلميات البحث أو النفاذ إلى نظام كمبيوتر أو إلى جزء منه، وفقاً للفقرة (1) (أ) وتوفر أسس لديها للاعتقاد بأن البيانات المطلوبة مخزنة داخل نظام كمبيوتر آخر أو على جزء منه على أراضي الدولة الطرف، وأنه يمكن النفاذ إلى تلك البيانات أو أنها متاحة قانونياً على النظام الأصلي، ينبغي أن تتمكن السلطات من تعجيل توسيع نطاق البحث أو النفاذ إلى النظام الآخر.

-3 تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من مصادرة أو تأمين بيانات الكمبيوتر التي تم النفاذ إليها طبقاً للفقرتين (1) أو (2). وتشمل هذه الإجراءات سلطة:

أ. مصادرة أو تأمين نظام الكمبيوتر أو جزء منه أو دعامة تخزين بيانات الكمبيوتر.

ب. إجراء نسخة من هذه البيانات الحاسوبية والاحتفاظ بها.

ج. الحفاظ على سلامة بيانات الكمبيوتر المخزنة ذات الصلة.

د. جعل تلك البيانات الحاسوبية غير قابلة للنفاذ على نظام الكمبيوتر الذي تم الولوج إليه أو إزالتها.

-4 تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من أمر أي شخص لديه معرفة بتشغيل نظام الكومبيوتر أو التدابير المطبقة لحماية البيانات الحاسوبية الموجودة عليه، بتقديم، في حدود المعقول، المعلومات اللازمة لتمكين إجراء التدابير المشار إليها في الفقرتين (1 و 2).

-5 تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و15).

الفصل الخامس: جمع بيانات الكمبيوتر في الوقت الحقيقي

المادة 20- جمع بيانات الكمبيوتر في الوقت الحقيقي

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية، على أراضيها.

ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة على:

1. جمع أو تسجيل من خلال تطبيق وسائل فنية، أو أراضي الدولة الطرف.

2. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات الحركة، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

2- في حال تعذر على الدولة الطرف، بسبب المبادئ القائمة في نظامها القانوني الوطني تبني التدابير المشار إليها في الفقرة (1) (أ)، يجوز لها بدلاً من ذلك اعتماد تدابير تشريعية وغيرها من التدابير الضرورية لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات الحركة المرتبطة باتصالات محددة تم نقلها على أراضيها، من خلال تطبيق وسائل فنية على تلك الأراضي.

3- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالحفاظ على سرية تنفيذ أي من السلطات المنصوص عليها في هذه المادة وعلى أي معلومات مرتبطة بها.

4- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و15).

المادة 21 - اعتراض بيانات المحتوى

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير، فيما يتعلق بنطاق الجرائم الجسيمة التي يحددها القانون الوطني، لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها.

ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة، على:

1. جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها.

2. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات المحتوى، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

2- في حال تعذر على الدولة الطرف تبني الإجراءات المشار إليها في الفقرة (1) (أ)، بسبب المبادئ القائمة في نظامها القانوني الوطني، يجوز لها بدلاً من ذلك أن تعتمد ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصالات معينة تم نقلها في أقاليمها عبر تطبيق وسائل فنية في تلك الأقاليم.

3- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالمحافظة على سرية تنفيذ أي من السلطات المنصوص عليها هذه المادة وأي معلومات متصلة بها.

4- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين (14 و15).

الباب الثالث: الولاية القضائية

المادة 22 - الولاية القضائية

1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على أي جريمة تنص عليها المواد من (2) إلى (11) من هذه الاتفاقية، عندما تُرتكب الجريمة:

أ. داخل أقاليمها.

ب. على متن سفينة ترفع علم تلك الدولة الطرف.

ج. على متن طائرة مسجلة بموجب قوانين تلك الدولة الطرف.

د. من قبل أحد مواطنيها، إذا كانت الجريمة مُعاقباً عليها بموجب القانون الجنائي في مكان ارتكابها أو في حال ارتكاب الجريمة خارج الولاية القضائية الإقليمية لأي دولة.

2- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم التطبيق أو التطبيق فقط في حالات أو ظروف معينة قواعد الولاية القضائية

المنصوص عليها في الفقرات من (1) (ب) إلى (1) (د) من هذه المادة أو أي جزء منها.

3- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على الجرائم المشار إليها في الفقرة (1) من المادة (24) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم متواجداً داخل أقاليمها ولا تقوم بتسليمه إلى دولة طرف أخرى على أساس جنسيته فقط، وذلك بعد التوصل بطلب التسليم.

4- لا تستبعد هذه الاتفاقية ممارسة أي دولة طرف لولاية جنائية يقرها قانونها الوطني.

5- في حال مطالبة أكثر من دولة طرف بالولاية القضائية على جريمة تقرها هذه الاتفاقية، تقوم الدول الأطراف المهنية، عند الاقتضاء، بالتشاور بغرض تحديد الولاية القضائية الأنسب للمقاضاة.

الباب الثالث: التعاون الدولي

القسم الأول: المبادئ العامة

الفصل الأول: المبادئ العامة ذات الصلة بالتعاون الدولي

المادة 23 – المبادئ العامة ذات الصلة بالتعاون الدولي

تتعاون الدول الأطراف فيما بينها، وفقاً لأحكام هذا الباب ومن خلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولي في المسائل الجنائية وبالترتيبات المتفق عليها بمقتضى التشريعات الموحدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية، على أوسع نطاق ممكن لأغراض إجراءات التحقيقات أو المتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر، أو من أجل جمع أدلة بشأن جريمة جنائية في شكل إلكتروني.

الفصل الثاني: المبادئ ذات الصلة بتسليم المجرمين

المادة 24 - تسليم المجرمين

1- أ. تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد من (2 إلى 11) من هذه الاتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد.

ب. في حال كانت هناك تقرير تطبيق عقوبة دنيا مختلفة بموجب ترتيبات متفق عليها على أساس تشريع موحد أو ذي الصلة بالمعاملة بالمثل أو بموجب معاهدة تسليم المجرمين، بما في ذلك الاتفاقية الأوروبية بشأن تسليم المجرمين (سلسلة المعاهدات الأوربية رقم 24)، واجبة التطبيق بين طرفين أو

أكثر، تُطبق العقوبة الدنيا المنصوص عليها بموجب تلك الترتيبات أو المعاهدة

2- تعتبر الجرائم الجنائية الواردة في الفقرة (1) من هذه المادة مدرجة كجرائم يجب فيها التسليم في أي معاهدة بشأن تسليم المجرمين قائمة بين الأطراف، وتتعهد الدول الأطراف بتضمين هذه الجرائم على أنها جرائم يجب فيها تسليم المجرمين في أي معاهدة بشأن تسليم المجرمين يتم إبرامها فيما بينهم.

3- في حالة تلقت دولة طرف تخضع تسليم المجرمين لشرط وجود معاهدة ذات الصلة طلباً بالتسليم من طرف دولة طرف أخرى لا تربطها بها معاهدة لتسليم المجرمين، يجوز لتلك الدولة الطرف اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم فيما يتعلق بأي من الجرائم الجنائية المشار إليها في الفقرة (1) من هذه المادة.

4- تعترف الدول الأطراف التي لا تشترط وجود معاهدة لتسليم المجرمين بالجرائم الجنائية المشار إليها في الفقرة (1) من هذه المادة على أنها جرائم يجب فيها تسليم المجرمين فيما بينها.

5- يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم أو معاهدات تسليم المجرمين واجبة التطبيق، بما في ذلك الأسباب التي تستند إليها الدولة الطرف المطالبة بالتسليم لرفض التسليم.

6- في حال رفض التسليم بشأن إحدى الجرائم المشار إليها في الفقرة (1) من هذه المادة، على أساس جنسية الشخص المطلوب فقط أو لأن الدولة الطرف المطلوب منها التسليم تعتبر أنها ذات الولاية القضائية على تلك الجريمة، تقوم الدولة الطرف المطلوب منها التسليم، بناء على طلب الدولة الطرف مقدمة الطلب، بإحالة القضية على سلطاتها المختصة بغرض المقاضاة ثم بإبلاغ الطرف الطالب بالنتيجة النهائية في الوقت المناسب. وتتخذ تلك السلطات قرارها وتُجري التحقيقات والمتابعات بنفس الطريقة المطبقة على أي جريمة أخرى ذات طابع مشابه بموجب القانون تلك الدولة الطرف

7- أ. تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر الاعتقال الاحترازي في حال عدم وجود معاهدة تسليم المجرمين.

ت. يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات التي يعينها الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت

المادة 25- المبادئ العامة ذات الصلة بالمساعدة المتبادلة

1- توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر أو بجمع أدلة جريمة جنائية في شكل إلكتروني.

2- تعتمد أيضاً كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتنفيذ الالتزامات الواردة في المواد من (27) إلى (35).

3- يجوز لكل دولة طرف، في الظروف العاجلة، المطالبة بالمساعدة المتبادلة أو بوثائق عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، بقدر ما توفره تلك الوسائل من مستويات ملائمة للأمن والتحقق من صحة البيانات (بما في ذلك استخدام التشفير عند الضرورة) مع التأكيد الرسمي بتطبيق تلك الوسائل عندما تطالب بذلك الدولة الطرف المطلوب منه تقديم المساعدة. وتقبل الدولة الطرف المطلوب منها تقديم المساعدة وتستجيب للطلب بأي من وسائل الاتصال العاجلة.

4- باستثناء ما تنص عليه تحديدا خلاف ذلك مواد هذا الباب، تخضع المساعدة المتبادلة للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها المساعدة، أو معاهدات المساعدة المتبادلة الجاري بها العمل بما في ذلك الأسس التي ترتكز إليها الدولة الطرف

المطلوب منها المساعدة لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها المساعدة ممارسة الحق في رفض المساعدة المتبادلة فيما يتعلق بالجرائم المشار إليها في المواد من (2) إلى (11) فقط على أساس أن الطلب يتعلق بجريمة تعتبرها جريمة مالية.

5- متى كان مسموحاً للدولة الطرف المطلوب منها المساعدة، طبقاً لأحكام هذا الباب، بتقديم المساعدة المتبادلة في حال وجود جريمة مزدوجة، يُعتبر هذا الشرط مستوفياً بغض النظر عما إذا كانت قوانينها تدرج الجريمة داخل التصنيف ذاته أو تطلق على الجريمة نفس المصطلح للطرف مقدم الطلب، طالما أن السلوك الذي يحدد الجريمة المطلوب تقديم المساعدة بشأنها يشكل جريمة جنائية بموجب قوانينها.

المادة 26 – المعلومات التلقائية

1- يجوز لدولة طرف، في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجزها في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررة طبقا لهذه الاتفاقية أو أن ذلك قد يؤدى إلى تقديم طلب للتعاون من جانب تلك الدولة الطرف بموجب هذا الباب.

2- يجوز للطرف الذي يقدم هذه المعلومات، قبل تقديمها، أن يطلب الحفاظ على سرية تلك المعلومات أو استخدامها فقط وفقاً لشروط مُعينة. وإذا لم يكن بإمكان الدولة الطرف المتلقية لهذه المعلومات الامتثال لهذا الطلب، وجب عليها إشعار الطرف المقدم للمعلومات بذلك، والذي يقرر عندئذ إذا ما كان يتعين عليه مع ذلك تقديم تلك المعلومات. في حال قبول الدولة الطرف المتلقية بالمعلومات الخاضعة للشروط، وجب عليها الالتزام بها.

الفصل الرابع: الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

المادة 27 – الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

1- في حالة عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد ومتعلق بمبدأ المعاملة بالمثل بين الدولة الطرف المقدمة للطلب والدولة الطرف المطلوب منها، تطبق أحكام الفقرات من (2) إلى (9) من هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة أو ترتيب أو تشريع من هذا القبيل، ما لم توافق الأطراف المعنية على تطبيق أي أو كل البنود الباقية من هذه المادة بدلا منها.

2- أ. تقوم كل دولة طرف بتعيين سلطة أو سلطات مركزية مسؤولة عن إرسال طلبات المساعدة المتبادلة والرد عليها، أو تنفيذها أو إحالتها على الجهات المختصة من أجل تنفيذها.

ب. تتواصل السلطات المركزية مع بعضها البعض بشكل مباشر.

ج. تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا بأسماء وعناوين السلطات المعينة طبقاً لهذه الفقرة.

د. يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات المركزية التي تعينها الدول الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت

3- يتم تنفيذ الطلبات الخاصة بالمساعدة المتبادلة بموجب هذه المادة وفقاً للإجراءات التي يحددها الطرف مقدم الطلب، فيما عدا ما يتعارض مع القانون الدولة الطرف المطلوب منها المساعدة.

4- يجوز للدولة الطرف المطلوب منها المساعدة، علاوة على أسس الرفض الواردة في الفقرة (4) من المادة (25)، أن ترفض تقديم المساعدة في حال:

أ. كان الطلب يتعلق بجريمة تعتبرها الدولة الطرف المطلوب منها المساعدة جريمة سياسية أو جريمة لها علاقة بجريمة سياسية.

ب. ارتأت تلك الدولة أن تنفيذ الطلب من المحتمل أن يمس بسيادتها، أمنها، نظامه العام، أو بمصالح أساسية أخرى.

5- يجوز للدولة الطرف المطلوب منها تقديم المساعدة تأجيل البث في الطلب إذا كان من شأن ذلك إلحاق الضرر بتحقيقات أو متابعات جنائية تنجزها سلطاتها.

6- قبل رفض أو تأجيل تقديم المساعدة، تقوم الدولة الطرف المطلوب منها تقديم المساعدة، عند الاقتضاء وبعد التشاور مع الدولة الطرف مقدمة الطلب، بالنظر في إمكانية تنفيذ الطلب جزئياً أو إخضاعه للشروط التي تراها ضرورية.

7- تخبر الدولة الطرف المطلوب منها تقديم المساعدة على الفور الدولة الطرف مقدمة الطلب بنتيجة تنفيذ الطلب الخاص بالمساعدة. ويتوجب شرح الأسباب أي رفض أو تأجيل للطلب. علاوة على ذلك، تخبر الدولة الطرف المطلوب منها المساعدة الطرف مقدم الطلب بالأسباب التي تجعل تنفيذ الطلب مستحيلا أو التي من المحتمل أن تؤخره بشكل هام.

8- يجوز للدولة الطرف مقدمة الطلب أن تطلب من الطرف المطلوب منه المساعدة الحفاظ على سرية أي طلب يتم تقديمه بموجب هذا الباب علاوة على موضوع الطلب، إلا في حدود ما هو ضروري

لتنفيذه. وفي حالة تعذر على الدولة الطرف المطلوب منها المساعدة الامتثال للطلب الخاص بالسرية، وجب عليها فورا إخبار الطرف مقدم الطلب الذي يقرر عندئذ ما إذا كان يتعين مع ذلك تنفيذ الطلب.

9- أ. في الحالات الطارئة، يجوز للسلطات القضائية بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات الخاصة بالمساعدة المتبادلة أو المراسلات المتعلقة بذلك إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة. وفي مثل هذه الحالات، يتم إرسال نسخة في الوقت نفسه إلى السلطة المركزية في الدولة الطرف المطلوب منها المساعدة عن طريق نظيرتها في الدولة الطرف مقدمة الطلب.

ب. يجوز تقديم أي طلب أو مراسلة بموجب هذه الفقرة من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول).

ج. في حال تقديم طلب وفقاً للفقرة الفرعية (أ) من هذه المادة وعدم اختصاص السلطة للتعامل مع الطلب، وجب على تلك السلطة إحالة الطلب على السلطة الوطنية المختصة وإخبار الدولة الطرف مقدمة الطلب فور إنجاز الإحالة.

د. يجوز للسلطات المختصة بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات أو المراسلات بموجب هذه الفقرة والتي

لا تتضمن أي إجراء إلزامي إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة

هـ يجوز لكل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق أو القبول، الموافقة أو الانضمام، إخبار الأمين العام لمجلس أوروبا أن الطلبات المقدمة بموجب هذه الفقرة يجب أن ترسل، من أجل الفعالية، إلى سلطتها المركزية.

المادة 28 - السرية والقيود على الاستخدام

1- في حال عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد أو المعاملة بالمثل بين الدولة الطرف مقدمة الطلب والدولة الطرف المطلوب منها المساعدة، تطبق أحكام هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة، ترتيب أو تشريع من هذا القبيل، ما لم تتفق الأطراف المعنية على تطبيق أي من البنود المتبقية من هذه المادة أو كلها بدلاً منها.

2- يجوز للدولة الطرف المطلوب منها المساعدة تقييد توفير المعلومات أو المواد في إطار تلبية الطلب المقدم بشرط:

أ. الحفاظ على سريتها في حال تعذر إمكانية الاستجابة لطلب المساعدة القانونية المتبادلة في غياب شرط من هذا القبيل.

ب. عدم استخدامها في تحقيقات أو إجراءات غير تلك المشار إليها في الطلب.

3- في حال تعذر على الدولة الطرف مقدمة الطلب الامتثال لأحد الشرطين المشار إليهما في الفقرة (2)، وجب عليها فوراً إخبار الطرف الآخر، الذي يقرر عندئذ إذا كان يتعين، مع ذلك، تقديم المعلومات. وفي حال قبول الدولة الطرف مقدمة الطلب لهذا الشرط، وجب عليها الالتزام به.

4- يجوز لأي دولة طرف تقدم معلومات أو مواد وفقاً لأحد الشروط المشار إليها في الفقرة (2) أن تطلب من الطرف الآخر توضيح استخدام تلك المعلومات أو المواد علاقة بذلك الشرط.

القسم الثاني: أحكام خاصة

الفصل الأول: المساعدة المتبادلة بشأن التدابير المؤقتة

المادة 29 - التعجيل في حفظ بيانات الكومبيوتر المخزنة

1- يجوز لأي دولة طرف أن تطالب دولة طرفا أخرى أن تأمر أو تحصل بطريقة أخرى على التعجيل في حفظ بيانات مُخزنة بواسطة نظام كمبيوتر، يوجد على أراضي الدولة الطرف الأخرى، والتي تنوي أن تقدم بشأنها طلباً بالمساعدة المتبادلة من أجل البحث عن بيانات، النفاذ إليها، مصادرتها، تأمينها أو كشفها.

2- يجب أن يحدد طلب الحفظ الذي يتم تقديمه بموجب الفقرة (1) ما يلي:

أ. الجهة التي تطلب الحفظ.

ب. الجريمة موضوع التحقيقات أو الإجراءات الجنائية وملخص موجز عن الوقائع المتعلقة بها.

ج. بيانات الكومبيوتر المخزنة المطلوب حفظها وعلاقتها بالجريمة.

د. أي معلومات متاحة تكشف عن القيِّم على بيانات الكومبيوتر المخزنة أو عن مكان وجود نظام الكمبيوتر.

هـ. الضرورة الموجبة للحفظ.

و. أن تلك الدولة تنوي تقديم طلب المساعدة المتبادلة من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها.

3- عند استلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه المساعدة باتخاذ كافة الإجراءات الملائمة وذلك لتعجيل حفظ البيانات المحددة وفقاً للقانون الوطني. ولأغراض الاستجابة للطلب، لا يجوز تقييد توفير هذا الحفظ بشرط ازدواجية التجريم.

4- يجوز لأي دولة طرف تقيد الاستجابة لطلب المساعدة المتبادلة بشرط ازدواجية التجريم من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها، بالنسبة لجرائم غير تلك المنصوص عليها وفقاً للمواد من (2) إلى (11) من هذه الاتفاقية، أن تحتفظ بالحق في رفض طلب الحفظ بموجب هذه المادة في الحالات التي يتوافر لديها فيها أسباب للاعتقاد بأنه يتعذر، في وقت الكشف أو الإفصاح عن هذه المعلومات، استيفاء الشرط الخاص بازدواجية التجريم.

5- بالإضافة إلى ذلك، يجوز رفض طلب الحفظ فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو جريمة مرتبطة بجريمة سياسية.

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

6- في حال اعتقاد الدولة الطرف المطلوب منها المساعدة أن الحفظ لن يضمن توافر البيانات مستقبلاً أو أنه سيهدد السرية أو يلحق الضرر بالتحقيقات التي تنجزها الدولة الطرف مقدمة الطلب، وجب عليها فوراً إخبار الدولة الطرف مقدمة الطلب التي يحدد عندئذ إذا ما كان ينبغي، مع ذلك، تنفيذ الطلب.

7- يكون أي حفظ يتم تفعيله استجابة للطلب المشار إليه في الفقرة (1) لفترة لا تقل عن ستين يوماً بغية تمكين الدولة الطرف مقدمة الطلب من تقديم طلب للبحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها. بعد تلقي طلب من هذا القبيل، يجب مواصلة حفظ البيانات في انتظار صدور قرار بشأن ذلك الطلب.

المادة 30 – تعجيل الكشف عن بيانات الحركة المحفوظة

1- في حال اكتشفت الدولة الطرف المطلوب منها المساعدة، أثناء تنفيذ طلب مقدم وفقاً للمادة (29) بحفظ بيانات الحركة المتعلقة باتصال

محدد، أن أحد مزودي الخدمة في دولة أخرى مشترك في نقل الاتصال، تقوم الدولة الطرف المطلوب منها المساعدة على الفور بالكشف عن القدر الكافي من بيانات الحركة لتحديد هوية مزود الخدمة والمسار الذي تم من خلاله ذلك الاتصال.

2- يجوز حجب بيانات الحركة بموجب الفقرة (1) فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو أنها متصلة بجريمة سياسية.

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

الفصل الثاني: المساعدة المتبادلة ذات الصلة بسلطات التحقيقات

المادة 31 – المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة

1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها عندما تكون تلك البيانات مخزنة بواسطة نظام كومبيوتر يوجد داخل أراضي الدولة الطرف المطلوب منها المساعدة، بما في ذلك البيانات التي تم حفظها وفقاً للمادة (29).

2- تستجيب الدولة الطرف المطلوب منها المساعدة للطلب من خلال تطبيق الصكوك والترتيبات والقوانين الدولية المشار إليها في المادة (23)، وطبقاً للأحكام الأخرى ذات الصلة الواردة في هذا الباب.

3- تتم الاستجابة للطلب بشكل معجل عندما:

أ. توجد أسباب للاعتقاد بأن البيانات ذات الصلة مُعَرضة بصفة خاصة للضياع أو التعديل.

ب. تكون الصكوك والترتيبات والقوانين المشار إليها في الفقرة (2) تنص على التعجيل في التعاون.

المادة 32 - النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم

يجوز لدولة طرف، دون ترخيص من دولة طرف أخرى:

أ. النفاذ إلى بيانات كمبيوتر مُخزنة متاحة للعموم (مصدر مفتوح) بغض النظر عن مكان تواجد البيانات جغرافياً.

ب. النفاذ إلى بيانات كمبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كمبيوتر داخل أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكمبيوتر المذكور.

المادة 33 – المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي

1- تقدم الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات الحركة في الوقت الحقيقي المرتبطة باتصالات محددة في أقاليمها والتي يتم نقلها بواسطة نظام كمبيوتر. وطبقاً لأحكام الفقرة (2)، تخضع هذه المساعدة للشروط والإجراءات المنصوص عليها بموجب القانون الوطني.

2- توفر كل دولة طرف مساعدة من هذا القبيل على الأقل فيما يتعلق بالجرائم الجنائية التي يكون فيها جمع بيانات الحركة في الوقت الحقيقي متاحاً في قضية محلية مماثلة.

المادة 34 – المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى

توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات المحتوى في الوقت الحقيقي أو تسجيلها فيما يتعلق باتصالات محددة يتم نقلها بواسطة نظام كمبيوتر بقدر ما تسمح به المعاهدات والقوانين الوطنية واجبة التطبيق.

المادة 35 – شبكة على مدار الساعة و (7) أيام في الأسبوع

1- تعين كل دولة طرف نقطة اتصال متاحة على مدار الساعة وسبعة أيام في الأسبوع بغية ضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني. وتشمل هذه المساعدة تسهيل، أو إذا كان قانونها الوطني وممارستها يسمح بذلك، تنفيذ التدابير التالية بشكل مباشر:

أ. توفير المشورة الفنية.

ب. حفظ البيانات طبقاً للمادتين (29) و (30)؛

ج. جمع الأدلة وتوفير المعلومات القانونية وتحديد موقع المشتبه بهم.

2- أ. يجب أن تتوفر نقطة الاتصال للدولة الطرف على القدرة على إجراء اتصالات مع مثيلتها في دولة طرف أخرى على وجه السرعة.

ب. إذا كانت نقطة الاتصال التي تعينها دولة طرف ليست جزءاً من السلطة أو السلطات المسؤولة عن المساعدة المتبادلة الدولية أو عن تسليم المجرمين، وجب على نقطة الاتصال

أن تضمن أنها قادرة على التنسيق مع تلك السلطة أو السلطات على وجه السرعة.

2- تضمن كل دولة طرف توفير طاقم حاصل على التدريب والمعدات الضروريين من أجل تسهيل تشغيل الشبكة.

الباب الرابع: الأحكام الختامية

المادة 36 – التوقيع ودخول حيز النفاذ

1- تفتتح هذه الاتفاقية للتوقيع من قبل الدول الأعضاء بمجلس أوروبا والدول غير الأعضاء التي شاركت في صياغتها.

2- تخضع هذه الاتفاقية للتصديق، القبول أو الموافقة. وتودع وثائق التصديق، القبول أو الموافقة لدى الأمين العام لمجلس أوروبا.

3- تدخل هذه الاتفاقية حيز التنفيذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ تعبير خمس دول، من بينها ثلاث دول على الأقل من أعضاء مجلس أوروبا، عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين (1 و2).

4- تدخل هذه الاتفاقية حيز التنفيذ، بالنسبة لأي دولة توقع عليها وتعرب بعدها عن موافقتها على الالتزام بها، في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ التعبير عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين (1 و 2).

المادة 37 – الانضمام إلى الاتفاقية

1- بعد دخول الاتفاقية حيز التنفيذ، يجوز للجنة وزراء مجلس أوروبا، بعد التشاور مع الدول المتعاقدة في الاتفاقية والحصول على موافقتها بالإجماع، توجيه الدعوة لأي دولة غير عضو في المجلس ولم تشارك في صياغة الاتفاقية للانضمام إلى هذه الاتفاقية. ويتم اتخاذ القرار بالأغلبية المنصوص عليها في المادة (20- د) من النظام الأساسي لمجلس أوروبا وعن طريق تصويت الدول المتعاقدة في الاتفاقية بالإجماع المخول لها المشاركة في لجنة الوزراء.

2- تدخل الاتفاقية حيز التنفيذ – بالنسبة لأي دولة تنضم للاتفاقية بموجب الفقرة (1) أعلاه – في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ إيداع وثيقة الانضمام لدى الأمين العام لمجلس أوروبا.

المادة 38 – التطبيق الإقليمي

1- يجوز لأي دولة، وقت التوقيع على الاتفاقية أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، تحديد الإقليم أو الأقاليم التي تطبق عليها هذه الاتفاقية.

2- يجوز لأي دولة، في أي تاريخ لاحق، وبموجب إعلان موجه إلى الأمين العام لمجلس أوروبا، توسيع نطاق تطبيق هذه الاتفاقية على أي إقليم يتم تحديده في الإعلان. وتدخل الاتفاقية حيز التنفيذ بالنسبة لهذا الإقليم في اليوم الأول من الشهر الموالي لانتهاء فترة

ثلاثة أشهر من تاريخ استلام الإعلان من قبل الأمين العام لمجلس أوروبا.

3- يجوز سحب أي إعلان تم تقديمه بموجب الفقرتين السابقتين، بالنسبة لأي إقليم محدد في مثل هذا الإعلان، بموجب إشعار موجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب الإعلان حيز النفاذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام لمجلس أوروبا لهذا الإشعار.

المادة 39 – الآثار المترتبة على الاتفاقية

1- يتلخص الغرض من هذه الاتفاقية في استكمال المعاهدات أو الترتيبات ثنائية أو متعددة الأطراف فيما بين الأطراف، بما في ذلك أحكام:

- الاتفاقية الأوروبية بشأن تسليم المجرمين، التي فتحت للتوقيع بباريس في 13 ديسمبر/ كانون الأول 1957م (سلسلة المعاهدات الأوروبية رقم 24).
- الاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية، التي فتحت للتوقيع بستراسبورغ في 20 أبريل/ نيسان 1959م (سلسلة المعاهدات الأوروبية رقم 30).
- البروتوكول الإضافي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية، التي فتحت للتوقيع

بستراسبورغ في 17 مارس/آذار 1978 (سلسلة المعاهدات الأوروبية رقم (99)).

2- في حال إبرام طرفين أو أكثر لاتفاقية أو معاهدة بشأن المسائل التي تتناولها هذه الاتفاقية، أو إقامة علاقات بشأن مثل هذه المسائل بشكل آخر، أو عزمهم القيام بذلك في المستقبل، تكون تلك الدول مخولة لتطبيق تلك الاتفاقية أو المعاهدة أو تنظيم علاقاتها بناء عليها. ومع ذلك، يجب على الدول الأطراف، في حال إقامة علاقات فيما يتعلق بالمسائل التي تتناولها هذه الاتفاقية بخلاف ما تنظمه هذه الاتفاقية، أن تنظم تلك العلاقات بطريقة تتفق مع أهداف الاتفاقية ومبادئها.

2- لا يؤثر أي شيء ورد بهذه الاتفاقية على حقوق أي دولة طرف، قيودها، التزاماتها ومسئولياتها.

المادة 40 – الإعلانات

يجوز لأي دولة، بموجب إعلان خطي يوجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، أن تعلن أنها تستفيد من إمكانية طلب عناصر إضافية كما هو منصوص عليه بموجب المواد (2، 3 و6) - الفقرة (1) (ب)، والمادة (7)، والمادة (9) - الفقرة (3)، والمادة (27) - الفقرة (9) (هـ).

المادة 41 – البند الاتحادي

1- يجوز للدولة الاتحادية الاحتفاظ بالحق في الاضطلاع بالالتزامات بموجب الباب الثاني من هذه الاتفاقية بما يتفق ومبادئها الأساسية التي تنظم العلاقة بين حكومتها المركزية والدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة شريطة أن تظل قادرة على التعاون بموجب الباب الثالث.

2- لا يجوز للدولة الاتحادية، عند التحفظ بموجب الفقرة (1)، تطبيق بنود هذا التحفظ لاستبعاد أو تقليص التزاماتها بشكل جوهري للتنصيص على التدابير المذكورة في الباب الثاني. وبشكل عام، يجب عليها توفير قدرة فعالة وواسعة في تنفيذ القانون فيما يتعلق بتلك التدابير.

3- بالنسبة لأحكام هذه الاتفاقية، التي يصبح تطبيقها بموجب الولاية القضائية للدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة غير الملزمة بالنظام الدستوري للاتحاد من أجل اتخاذ تدابير تشريعية، تقوم الحكومة الفيدرالية بإخبار السلطات المختصة في تلك الدول بالأحكام المذكورة إلى جانب رأيها المفضل، لتشجيعها على اتخاذ الإجراءات الملائمة لتفعيلها.

المادة 42 – التحفظات

يجوز لأي دولة، بموجب إشعار خطي موجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة

أو الانضمام، أن تعلن أنها تستفيد من التحفظ أو التحفظات المنصوص عليها في المادة (4) – الفقرة (2)، والمادة (6) – الفقرة 3، والمادة (9) – الفقرة (4)، والمادة (10) – الفقرة (3)، والمادة (11) – الفقرة (3)، والمادة (14) – الفقرة (3)، والمادة (22) – الفقرة (2)، والمادة (29) – الفقرة 4، والمادة (41) – الفقرة (1). ولا يجوز تقديم أية تحفظات أخرى.

المادة 43 - الوضع التحفظات وسحبها

1- يجوز لأي دولة طرف تقدمت بتحفظ طبقاً للمادة (42) أن تسحب ذلك التحفظ كلياً أو جزئياً وذلك عن طريق إشعار خطي موجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب التحفظ حيز التنفيذ في تاريخ استلام الإشعار من قبل الأمين العام لمجلس أوروبا. وفي حال أشار الإشعار إلى تاريخ محدد لدخول سحب التحفظ حيز النفاذ، وكان ذلك التاريخ لاحقاً لتاريخ استلام الإشعار من قبل الأمين العام، يبدأ العمل بسحب التحفظ في ذلك التاريخ اللاحق.

2- يجوز لأي دولة طرف تقدمت بتحفظ كما هو مشار إليه في المادة (42) سحب هذا التحفظ، كلياً أو جزئياً، بمجرد ما تسمح الظروف بذلك.

3- يجوز للأمين العام لمجلس أوروبا أن يستفسر، بشكل دوري، الدول الأطراف التي استخدمت تحفظا أو أكثر من تحفظ طبقاً للمادة (42) عن احتمالات سحب ذلك التحفظ (أو تلك التحفظات).

المادة 44 - التعديلات

1- يجوز لأي دولة طرف اقتراح تعديلات على هذه الاتفاقية، ويقوم الأمين العام لمجلس أوروبا بإرسالها إلى الدول الأعضاء بمجلس أوروبا، والدول غير الأعضاء التي شاركت في صياغة الاتفاقية، وكذلك إلى أي دولة انضمت إليها، أو تم توجيه الدعوة إليها للانضمام إلى هذه الاتفاقية وفقاً لأحكام المادة (37).

2- يرسل أي تعديل مقترح من قبل دولة طرف إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، التي تعرض رأيها في هذا التعديل المقترح على لجنة الوزراء.

3- تنظر لجنة الوزراء في التعديل المقترح والرأي الذي تحيله عليها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، ويجوز لها، بعد التشاور مع الدول الأطراف غير الأعضاء في هذه الاتفاقية، تبني التعديل.

4- يرسل نص أي تعديل تتبناه لجنة الوزراء طبقاً للفقرة (3) من هذه المادة إلى الدول الأطراف للموافقة عليه.

5- يدخل أي تعديل يتم إقراره طبقاً للفقرة (3) من هذه المادة حيز التنفيذ في اليوم الثلاثين بعد إخبار جميع الدول الأطراف الأمين العام لمجلس أوروبا بقبولها بذلك التعديل.

المادة 45 - تسوية النزاعات

1- يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم بما يتعلق بتفسير وتطبيق هذه الاتفاقية.

2- في حال حدوث نزاع بين دول أطراف بشأن تفسير أو تطبيق هذه الاتفاقية، يتيعن عليها السعي إلى تسوية للنزاع عبر التفاوض أو أي وسيلة سلمية أخرى من اختيارهم، بما في ذلك إحالة النزاع على اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) أو إلى هيئة تحكيم والتي تكون قرارتها ملزمة بالنسبة للأطراف، أو إلى محكمة العدل الدولية حسبما تتفق عليه الأطراف المعنيين.

المادة 46 – مشاورات الأطراف

1- تقوم الدول الأطراف، عند الاقتضاء، بالتشاور فيما بينها بشكل دوري بغية تيسير:

أ. الاستخدام والتنفيذ الفعال لهذه الاتفاقية، بما في ذلك تحديد أي مشاكل ذات الصلة، علاوة على آثار أي إعلان أو تحفظ يتم تقديمهما بموجب هذه الاتفاقية.

ب. تبادل المعلومات بشأن التطورات القانونية، السياسية أو التكنولوجية ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في شكل إلكتروني.

ج. دراسة الإضافات أو التعديلات الممكنة للاتفاقية.

2- يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم، بشكل دوري، بنتائج المشاورات المشار إليها في الفقرة (1).

3- تقوم اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، عند الاقتضاء، بتيسير المشاورات المشار إليها في الفقرة (1) واتخاذ التدابير اللازمة لمساعدة الدول الأطراف في جهودها لاستكمال أو تعديل الاتفاقية. وتقوم اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، على الأكثر بعد ثلاث سنوات من دخول هذه الاتفاقية حيز التنفيذ، بالتعاون مع الدول الأطراف لإجراء مراجعة لكافة أحكام الاتفاقية، وعند الضرورة، تقدم توصيات بالتعديلات الملائم.

4- بخلاف ما يتكفل به مجلس أوروبا، تلتزم الدول الأطراف بالنفقات الناجمة عن تنفيذ أحكام الفقرة (1) بالطريقة التي تحددها.

5- تساعد الأمانة العامة لمجلس أوروبا الدول الأطراف في تنفيذ مهامها طبقاً لهذه المادة.

المادة 47 - الانسحاب

1- يجوز لأي دولة طرف، في أي وقت، الانسحاب من هـذه الاتفاقيـة عـن طريق إشعار موجه إلى الأمين العام لمجلس أوروبا.

2- ويدخل هذا الانسحاب حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام للإشعار.

المادة 48 - الإبلاغ

يقوم الأمين العام لمجلس أوروبا بإبلاغ الدول الأعضاء في مجلس أوروبـا والدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية، علاوة على أي دولة انضمت إليها أو دعيت للانضمام إلى هذه الاتفاقية بما يلي:

أ. أي توقيع.

ب. إيداع أي صك للتصديق، القبول، الموافقة أو الانضمام.

ج. أي تاريخ لدخول هذه الاتفاقيـة حيـز التنفيـذ طبقـاً للمادتـين (36) و (37)؛ د.أي إعلان يتم تقديمـه بموجـب المـادة (40) أو أي تحفـظ يـتم تقديمه طبقاً للمادة (42).

هـ أي إجراء، إخطار أو تواصل آخر يتعلق بهذه الاتفاقية.

وإثباتاً لذلك، قام الموقعون أدناه، المفوضون بـذلك حسـب الأصـول، بـالتوقيع على هذه الاتفاقية.

حرر في بودابست - في الثالث والعشريـن مـن شـهر نـوفمبر/ تشريـن الثاني 2001م، باللغتين الإنجليزية والفرنسية وكلا النصين متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا. ويرسل الأمين العـام لمجلس أوروبا نسخا مصدقا عليها إلى كل دولة عضـو في مجلـس أوروبـا، وإلى الدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية وإلى أي دولة دعيـت للانضمام إليها.

قائمة المصادر والمراجع

أولاً: المصادر والمراجع العربية

1- ابن منظور، محمد بن مكرم (711هـ)، لسان العرب، ط1، دار صادر، بيروت، 2000م، ج1.

2- الاتفاقية المتعلقة بالجريمة الإلكترونية بودابست 2001م، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم (185)

3- جبور، منى الأشقر، الأمن السيبراني: التحديات ومستلزمات المواجهة "اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني"، جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية، 2012م.

4- الحلو، عزيز نور، الإرهاب في القانون الدولي: دراسة قانونية مقارنة، 2007م.

5- حومد، عبد الوهاب، الحقوق الجزائية العامة، دمشق، 1956م.

6- دولي أحمد، الإرهاب الدولي، مطبعة صادر، 2004م، بيروت.

7- زرقط، عمر، "اختصاص المحكمة الجنائية الدولية في نظر جرائم الإرهاب"، 2017م.

8- الشكري، عادل يوسف عبد النبي، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة، العراق، جامعة الكوفة، العدد السابع 2008م.

9- صالح، محمود، (2006م)، الجرائم المعلوماتي، مسقط: ورقة عمل قدمت إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية عقد بسلطنة عُمان. في الفترة (42)، أبريل، 2006م.

10- صلاح الدين، عامر، المقاومة المسلحة في القانون الدولي العام، دار الفكر العربي، رسالة دكتوراه، جامعة القاهرة، 1977م.

11- عبد الصادق، عادل، الإرهاب الإلكتروني، " القوة في العلاقات الدولية نمط جديد"، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، 2009م، ط1.

12- عطا محمد زهرة، في الأمن القومي العربي، منشورات جامعة قار يونس، 1991م.

13- الغافري، حسين بن سعيد، (2011م)، الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، مسقط: بحث مقدم لكلية الحقوق، جامعة السلطان قابوس في الفترة من 13-2011/3/14م.

14- فريد، نائلة عادل محمد، (2005م)، جرائم الحاسب الاقتصادية، القاهرة، دار النهضة العربية.

15- القرار الصادر عن الجمعية العامة للأمم المتحدة في 20 نوفمبر عام 2000م، الرقم 55/28.

16- الكيالي، عبد الوهاب، موسوعة السياسة، ج1، ط2، الموسوعة العربية للدراسات والنشر، بيروت 1985م.

17- معوض، جلال، ندوة العنف السياسي، مجلة المستقبل العربي، العدد 110، تموز 1987م.

18- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا عام 2013م، الوثيقة: UNODC/CCOCJ/EG.4/2013/2

19- منظمة الأسكوا، الإرشاد الخامس للأسكوا، 2011م.

20- مولود، رنا سبع، ماهية الإرهاب وتأثيره على واقع حقوق الإنسان فينا وبريطانيا أنموذجاً، مركز الدراسات الاستراتيجية والدولية،، جامعة بغداد، 2011م.

21- المويشير، تركي عبد الرحمن، (2009م)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، رسالة دكتوراه في العلوم الأمنية، الرياض: جامعة نايف العربية للعلوم الأمنية.

22- النقوزي، عبد القادر زهير، المفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات الحلبي الحقوقية، 2008م.

23- النقوزي، عبد القادر زهير، **المفهوم القانوني لجرائم الإرهاب الداخلي والدولي**، منشورات الحلبي الحقوقية، الطبعة (1)، 2008م، بيروت، لبنان.

ثانياً: الموقع الإلكتروني:

1- **https://www.tripwier.com/state-of-security/goverment.**

2- https://www.weforum.org/agenda/2016/06/coulda-cyber-attack-cause-a-financial-crisis.

3- http//www.sytimes.com/2009/06/28/world/28cyber.html?_r_1&scp=3&cp=Vladislay%20sherstyuk& st=cse; accessed June 7,2010.

4- **UN and ITU team up to fight Cybercrime** By Messaging News staff

5- مؤتمر الإنتربول واليورو بول الثاني للجريمة الإلكترونية سنغافورة 3-1 أكتوبر 2014م (INTERPOL/EUROPOL Cybercrime Conference

6- السند، عبد الرحمن بن عبد الله، **وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها** من الموقع: http://shamela.ws/browse.php/book-1244/page-20

7- https://www.itu.int/ar/ITU-D/Statisticsh.

8- Alix DESFORGES, “Cyberterrorisme : quel périmètre ?”, Fiche de l’Irsem n° 11, décembre 2011 , p.03. file:///C:/Users/sarra/Downloads/Fiche_n11_perimetre_cyberterrorisme%20(2).pdf 03/02/2017 à 08:39.

9- McConnell said the Internet has "introduced a level of vulnerability that is unprecedented".

Cybersecurity starts at home and in the office. http://www.google.com:80/hostednews/ap/article/ALeqM5gkZ5sKNT86kqT9TWeDlogVPoASyQD9B469980

10- Loppsi en France et Cyber-securite aux USA http://www.natchers.com/actualite-2009/8239/loppsi-en-france-et-cyber-securite-aux-usa

ثالثاً: المصادر والمراجع الأجنبية

1- President Obama's Remarks on Securing U.S. Cyber Infrastructure, " May 29, 2009, English/2009/May/20090529161700eaifas0.1335871/html.

2- Arguilla, J and D.Ronfeld", In Athena's Camp: Preparing for Conflict in the Information Age, Rand Publishing, Santa Monia, CA, USE, 1997.

3- Christoper C. Joyner & Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", Europe Journal of Infernatonal Law, vol, 12, 2001.

4- David Cameron, " How Britain can best address the threats of the twenty-first century", address at Chatham House, Lodon, 15 Jan, 2010. http://www.chathamhoure.org.uk. events/view/-/id/1419/. Accessed 20 Jan. 2010.

5- DOROTHY E. DENNING," Cyber terrorism" , **Global Dialogue**, Autumn, 2000.

6- Electronic money regulations 2011 (EMR 2011) & the payment Services Regulations 2009.

7- Franz-Stefan Gady and Greg Austin, " Russia, The United States, And Cyber Dipomacy Opening the Doors", The Eest West Institue, Printed in the United Stated. 2010.

8- James, A.Lewis, " Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, Spring Summer, Vol: XVI, Issue II, 2010.

9- Larry Wortzel, " China's Cyber-offensive", Wall Street Journal, I Nov, 2009.

10- Marco Roscini, " World Wide Warfare – Jus ad bellum and use of Cyber force", Max Planck Yearbook of United Nations Law. Volume 14. 2010.

11- Micheal S. Fuertes, " Cyber warfare, Unjust Actins in a just War", Florida International University, Full 2013.

12- Nathan E. Mueller, " Micheal Walzer on the Moral Legitimacy of states and the Morality of Killing in War", Thesis Submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts in Philosophy, May 10, 2006.

13- Schmitt, M.N, " Computer Network Attack and the Use of Force In International Law trough on A Normative", The Colomia Journal of Transitional Law, 1999, Vol, 27, No, 885-937.

14- Shin, Beomchul, " The Cyber Warfare and the Right of Self – Defense: Legal Perspectives and the Case of the United States,IFANS, Vol, 19, Nol. June 2011.

15- Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry, I. Grigoriev, Pavan Duggal , and Stein Schjolnerg, Global Cyber Deterrence Views from China, the U.S,. Russia, India, and Norway", The East West Institute, Printed in the United States, 2010, p3.

16- Trends in Telecommunication Reform 2010-11- ITU-" The term "cyber security" refers to various activities such as the collection of tools, policies,security safeguards, guidelines, risk management approaches, training, best practices, andtechnologies that can be used to protect the cyber environment and the assets of organizations and Users".

17- U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Pulication 1-02, Nov. 8, 2010, as amended through Feb, 15, 2012.

18- Yoram Dinstein, " Computer Network Attacks and Self-Defence", International Law Studies, Review, Vol. no. 99, 2002.

19- Zimet. E. and C. L. Barry, " Military services Overview, Cyber power and National Security", National Defense University Press, Washington, DC, USA, 2009.



الرواد والمرجع الأصدق للكتاب الجامعي الأكاديمي

دار زهران للنشر والتوزيع

تلفاكس: 0096265331289 ص.ب. :1170 عمان – الرمز البريدي: 11941 الأردن

E-mail: zahran.publishers@gmail.com www.zahranpublishers.com

